

Risk Management Series

# Reference Manual

to Mitigate Potential Terrorist Attacks Against Buildings

December 2003



**FEMA**



**RISK MANAGEMENT SERIES**

Reference Manual *to*  
Mitigate Potential Terrorist  
Attacks Against Buildings

**PROVIDING PROTECTION TO PEOPLE AND BUILDINGS**



**FEMA**

**Federal Emergency Management Agency**  
**[www.fema.gov](http://www.fema.gov)**

---





---

**T**he creation of the Department of Homeland Security (DHS) is one of the most significant transformations in the Federal Government in decades, establishing a department whose first priority is to protect the nation against terrorist attacks. Within the DHS, the Directorate of Emergency Preparedness and Response (EP&R) is focused on ensuring that our nation is prepared for catastrophes, including both natural disasters and terrorist assaults.

Central to this mission is the protection of people and the critical infrastructure of the built environment. This Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings provides guidance to the building science community of architects and engineers, to reduce physical damage to buildings, related infrastructure, and people caused by terrorist assaults.

The comprehensive approach to understanding how to improve security in high occupancy buildings will better protect the nation from potential threats by identifying key actions and design criteria to strengthen our buildings from the forces that might be anticipated in a terrorist assault. It is important to note that many of the methodologies in this publication have been adapted from other government sources and modified to meet the mission of the DHS. This allows for the effective transfer of decades of federal and Department of Defense research and experience to the broader building science community.

This document was prepared by the Building Sciences and Technology Branch of the Mitigation Division, part of EP&R. The DHS would like to thank the following agencies for their contribution and input to this publication:

- General Services Administration
- Naval Facilities Engineering Service Center
- Naval Facilities Command (NAVFAC) Criteria Office
- USACE Protective Design Center
- Department of Veterans Affairs
- Centers for Disease Control and Prevention/National Institute for Occupational Safety and Health
- Department of Justice, Office of Domestic Preparedness (DHS - Border and Transportation Security)
- United States Air Force - Civil Engineer Support Agency

**Michael D. Brown**  
Under Secretary  
Emergency Preparedness  
and Response Directorate

**Anthony S. Lowe**  
Director  
Mitigation Division  
Emergency Preparedness and Response Directorate

---



# FOREWORD AND ACKNOWLEDGMENTS

---

## BACKGROUND

The Federal Emergency Management Agency (FEMA) developed this *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings* to provide needed information on how to mitigate the effects of potential terrorist attacks. The intended audience includes the building sciences community of architects and engineers working for private institutions, and state and local government officials working in the building sciences community. The manual supports FEMA's Mission (Lead America to prepare for, prevent, respond to, and recover from disasters) and the Strategic Plan's Goal 3 (Prepare the Nation to address the consequences of terrorism), all of which will be done within the all-hazards framework and the needs of Homeland Security.

The building science community, as a result of FEMA's efforts, has incorporated extensive building science into designing and constructing buildings against natural hazards (earthquake, fire, flood, and wind). To date, the same level of understanding has not been applied to manmade hazards (terrorism/intentional acts) and technological hazards (accidental events). Since September 11, 2001, terrorism has become a dominant domestic concern. Security can no longer be viewed as a standalone capability that can be purchased as an afterthought and then put in place. Life, safety, and security issues must become a design goal from the beginning.

## OBJECTIVE AND SCOPE

The objective of this manual is to reduce physical damage to structural and non-structural components of buildings and related infrastructure, and also to reduce resultant casualties during conventional bomb attacks, as well as attacks using chemical, biological, and radiological (CBR) agents. Although the process is general in nature and applies to most building uses, this manual is most applicable for six specific types of facilities:

- Commercial office facilities
- Retail commercial facilities
- Light industrial and manufacturing facilities

- Health care facilities
- Local schools (K-12), and
- Higher education (university) facilities

The processes and measures may not generally be economical or applicable to lighter density occupancies, such as single-family homes. More intense occupancies (e.g., industrial facilities) have already been addressed in most cases.

This is one of a series of publications that address security issues in high-population, private sector buildings. This document is the foundation of the *Building Vulnerability Design Against Terrorist Attacks Training Course* (FEMA 438).

The purpose of this manual is to provide guidance to the building sciences community working for private institutions. It presents tools to help decision-makers assess the performance of their buildings against terrorist threats and to rank recommendations. It is up to the decision-makers to decide which types of threats they wish to protect against and to determine their level of risk to each threat. Those decision-makers who consider their buildings to be at high risk can use this guidance as necessary.

The information contained in this document is:

- not mandatory
- not applicable to all buildings
- not applicable when it interferes with other hazards such as fire

This manual presents incremental approaches that can be implemented over time to decrease the vulnerability of buildings to terrorist threats. Many of the recommendations can be implemented quickly and cost-effectively.

## **ASSUMPTIONS**

The information provided herein builds upon the synergies between the mitigation measures for natural hazards and man-made hazards. For example, seismic standards for non-structural building components are beneficial against the explosive blast of conventional bombs. Hurricane window design, especially against flying debris, applies also to explosive blast. Landscaping for mitigation against wildfires improves detection of placed devices. Ventilation system design against airborne biological, chemical, and radiological agents also works for similar hazardous material releases, whether intentional or accidental. Assessing threat, vulnerability, and risk may be complicated when comparing natural against manmade hazards. A natural hazard refers to a natural event such as a flood, wind, or seismic disaster. Historical data have been used by FEMA and other agencies/organizations to economically quantify the risk for natural hazards. Manmade hazards include technological hazards and terrorism and they are distinct from natural hazards primarily in that they originate from human activity. Technological hazards are assumed to be accidental and that their consequences are unintended. There is limited discussion of technological hazards in this document. For manmade hazards, the threat and likelihood of occurrence are less well defined and the associated vulnerabilities have many considerations that impact making good risk management decisions.

## **ORGANIZATION AND CONTENT OF THE MANUAL**

This manual contains many how-to aspects based upon current information contained in FEMA, Department of Commerce, Department of Defense (including Army, Navy, and Air Force), Department of Justice, General Services Administration, Department of Veterans Affairs, Centers for Disease Control and Prevention/National Institute for Occupational Safety and Health, and other publications. It is intended to provide an understanding of the current methodologies for assessing threat/hazard, vulnerability, and risk, and the design considerations needed to improve protection of new and existing buildings and the people occupying them. As needed, this manual should be

supplemented with more extensive technical resources, as well as the use of experts when necessary.

- Chapter 1 presents selected methodologies to integrate threat/hazard, asset value, and vulnerability assessment information. This information becomes the input for determining relative levels of risk. Higher risk hazards require mitigation measures to reduce risk. The chapter also provides an assessment checklist that compiles many best practices (based upon current technologies and scientific research) to consider during the design of a new building or renovation of an existing building. The checklist can also be used to assess the vulnerability of existing buildings within the context of the defined threats.
- Chapter 2 discusses architectural and engineering design considerations (mitigation measures), starting at the perimeter of the property line, and includes the orientation of the building on the site. Therefore, this chapter covers issues outside the building envelope.
- Chapter 3 provides the same considerations for the building – its envelope, systems, and interior layout.
- Chapter 4 provides a discussion of blast theory to understand the dynamics of the blast pressure wave, the response of building components, and a consistent approach to define levels of protection.
- Chapter 5 presents CBR measures that can be taken to mitigate vulnerabilities and reduce associated risks for these terrorist tactics or technological hazards.
- Appendices A, B, and C contain acronyms, general definitions, and CBR definitions, respectively.
- Appendix D describes electronic security systems and design considerations.

- Appendices E and F present a comprehensive bibliography of publications, and the associations and organizations capturing the building security guidance needed by the building sciences community, respectively.

## **ACKNOWLEDGMENTS**

### **Principal Authors:**

Michael Chipley, UTD, Inc.  
Michael Kaminskas, UTD, Inc.  
Wesley Lyon, UTD, Inc.  
David Beshlin, UTD, Inc.  
Mark Hester, UTD, Inc.

### **Consultant Project Manager:**

Eric Letvin, Greenhorne & O'Mara, Inc.

### **Contributors:**

Eve Hinman, ATC/Hinman Consulting Engineers, Inc.  
G. Scott Earnest, CDC/NIOSH  
Michael Gressel, CDC/NIOSH  
Kenneth Mead, CDC/NIOSH  
D. Shawn Fenn, FEMA  
Randall Hoffman, UTD, Inc.  
Damian Kolbay, UTD, Inc.  
Mark Hankewycz, Gage-Babcock, Inc.  
Christopher Arnold, Building Systems Development, Inc.  
Deb Daly, Greenhorne & O'Mara, Inc.  
Wanda Rizer, Greenhorne & O'Mara, Inc.  
Julie Liptak, Greenhorne & O'Mara, Inc.  
Bob Pendley, Greenhorne & O'Mara, Inc.  
Bill Modzeleski, Department of Education

**Project Advisory Panel:**

Wade Belcher, General Services Administration  
Curt Betts, U.S. Army Corps of Engineers  
Jim Caulder, U.S. Air Force – Civil Engineer Support Agency  
Marcelle Habibion, Department of Veterans Affairs  
Joseph Hartman, U.S. Army Corps of Engineers  
David Hattis, Building Technology, Inc.  
Rick Jones, Naval Facilities Engineering Service Center  
Kurt Knight, Department of Veterans Affairs  
Frederick Krimgold, Virginia Tech  
John Lynch, Naval Facilities Command (NAVFAC) Criteria Office  
Terry Pruitt, Department of Homeland Security  
Chris Rojahn, Applied Technology Council  
Lloyd Siegel, Department of Veterans Affairs  
William Whiddon, Building Technology, Inc.

**Project Manager:**

Milagros Kennett, FEMA, Building Sciences Technology Branch, Mitigation Division

This manual was prepared by Greenhorne & O'Mara, Inc., under contract to FEMA. It will be revised periodically, and comments and feedback to improve future editions are welcome.

Please send comments and feedback by e-mail to [riskmanagementseriespubs@dhs.gov](mailto:riskmanagementseriespubs@dhs.gov)



# TABLE OF CONTENTS

---

<b>FOREWORD AND ACKNOWLEDGMENTS .....</b>	<b>i</b>
Background.....	i
Objective and Scope .....	i
Assumptions .....	iii
Organization and Content of the Manual.....	iii
Acknowledgments.....	v
 <b>CHAPTER 1 – ASSET VALUE, THREAT/HAZARD, VULNERABILITY, AND RISK.....</b>	 <b>1-1</b>
1.1 Asset Value Assessment .....	1-10
1.1.1 Identifying Building Core Functions.....	1-11
1.1.2 Identifying Building Infrastructure .....	1-11
1.1.3 Quantifying Asset Value.....	1-12
1.2 Threat/Hazard Assessment.....	1-14
1.2.1 Threat/Hazard Identification.....	1-14
1.2.2 Threat Definition of Physical Attack on a Building.....	1-21
1.3 Vulnerability Assessment .....	1-24
1.4 Risk Assessment.....	1-35
1.5 Risk Management.....	1-42
1.6 Building Vulnerabilty Assessment Checklist .....	1-45
 <b>CHAPTER 2 – SITE AND LAYOUT DESIGN GUIDANCE .....</b>	 <b>2-1</b>
2.1 Land Use Considerations .....	2-2
2.2 Site Planning .....	2-6
2.2.1 Site Design.....	2-6
2.2.2 Layout and Form.....	2-6

2.2.3	Vehicular and Pedestrian Circulation .....	2-11
2.2.4	Infrastructures and Lifelines.....	2-13
2.2.5	Landscape and Urban Design.....	2-14
2.3	Stand-off Distance .....	2-22
2.4	Controlled Access Zones .....	2-25
2.4.1	Physical Protective Barriers .....	2-27
2.4.2	Other Perimeter Barriers .....	2-30
2.4.3	Anti-ram Vehicle Barriers .....	2-32
2.5	Entry Control and Vehicular Access .....	2-36
2.6	Signage.....	2-40
2.7	Parking.....	2-42
2.8	Loading Docks and Service Access .....	2-44
2.9	Physical Security Lighting.....	2-45
2.10	Site Utilities.....	2-47
2.11	Summary of Site Mitigation Measures.....	2-51
2.12	Crime Prevention Through Environmental Design (CPTED) .....	2-59
<b>CHAPTER 3 – BUILDING DESIGN GUIDANCE .....</b>		<b>3-1</b>
3.1	Architectural.....	3-3
3.1.1	Building Configuration .....	3-3
3.1.2	Space Design .....	3-6
3.1.3	Other Design Considerations .....	3-8
3.2	Building Structural and Nonstructural Systems .....	3-10
3.2.1	Building Design to Achieve a Desired Protection Level .....	3-10
3.2.2	Progressive Collapse .....	3-10

3.2.3	Loads and Stresses .....	3-13
3.2.4	Good Engineering Practice Guidelines.....	3-14
3.2.5	Building Materials.....	3-16
3.2.6	Methods and References .....	3-16
3.3	Building Envelope.....	3-17
3.3.1	Building Exterior .....	3-17
3.3.2	Exterior Wall Design .....	3-18
3.3.3	Window Design .....	3-20
3.3.4	Doors.....	3-31
3.3.5	Roof System Design .....	3-32
3.4	Mechanical Systems .....	3-33
3.5	Electrical Systems .....	3-44
3.6	Fire Protection Systems.....	3-45
3.7	Communications Systems.....	3-45
3.8	Electronic Security Systems .....	3-46
3.9	Entry-control Stations .....	3-48
3.10	Physical Security Systems .....	3-50
3.11	Summary of Building Envelope Mitigation Measures.....	3-50
<b>CHAPTER 4 – EXPLOSIVE BLAST.....</b>		<b>4-1</b>
4.1	Blast Effects.....	4-1
4.1.1	Building Damage .....	4-6
4.1.2	Injuries.....	4-8
4.1.3	Levels of Protection .....	4-8
4.2	Stand-off Distance and the Effects of Blast .....	4-13
4.3	Predicting Blast Effects .....	4-16

4.3.1	Blast Load Predictions .....	4-16
4.3.2	Blast Effects Predictions .....	4-18
 <b>CHAPTER 5 – CHEMICAL, BIOLOGICAL, AND RADIOLOGICAL MEASURES.....</b>		
		5-1
5.1	Evacuation .....	5-2
5.2	Sheltering in Place .....	5-2
5.3	Personal Protective Equipment .....	5-5
5.4	Air Filtration and Pressurization .....	5-7
5.4.1	Air Filtration and Cleaning Principles .....	5-8
5.4.2	Applying External Filtration .....	5-20
5.4.3	Applying Internal Filtration (Recirculation Filter Units) .....	5-24
5.4.4	Radiological Hazards .....	5-25
5.5	Exhausting and Purging .....	5-26
5.6	CBR Detection.....	5-26
5.7	Indications of CBR Contamination .....	5-31
 <b>APPENDIX A – Acronyms</b>		
 <b>APPENDIX B – General Glossary</b>		
 <b>APPENDIX C – Chemical, Biological, and Radiological Terms Glossary</b>		
 <b>APPENDIX D – Electronic Security Systems</b>		
 <b>APPENDIX E – Bibliography</b>		
 <b>APPENDIX F – Associations and Organizations</b>		

## TABLES

### Chapter 1

Table 1-1	Asset Value Scale.....	1-13
Table 1-2	Nominal Building Asset Value Assessment.....	1-14
Table 1-3	Event Profiles for Terrorism and Technological Hazards.....	1-17
Table 1-4	Homeland Security Threat Conditions .....	1-24
Table 1-5	Site/Building Inherent Vulnerability Assessment Matrix (Partial Risk Assessment) .....	1-25
Table 1-6	Classification Table Extracts .....	1-26
Table 1-7	Selected Extracts – Recommended Standards Chart.....	1-27
Table 1-8	Level of Visibility .....	1-29
Table 1-9	Criticality of Target Site .....	1-30
Table 1-10	Target Value to Potential Threat Element.....	1-30
Table 1-11	Aggressor Access to Target .....	1-31
Table 1-12	Target Threat of Hazard (WMD Materials) .....	1-31
Table 1-13	Site Population Capacity.....	1-32
Table 1-14	Potential for Collateral Damage (Mass Casualties) .....	1-32
Table 1-15	Building Summary Sheet.....	1-33
Table 1-16	Building Ranking .....	1-33
Table 1-17	Simplified Building Ranking Matrix.....	1-34
Table 1-18	Risk Factors Definitions .....	1-38
Table 1-19	Total Risk Color Code .....	1-38
Table 1-20	Site Functional Pre-Assessment Screening Matrix.....	1-38

Table 1-21	Site Infrastructure Systems Pre-Assessment Screening Matrix .....	1-39
Table 1-22	Building Vulnerability Assessment Checklist.....	1-46
<b>Chapter 2</b>		
Table 2-1	Correlation of Mitigation Measures to Threats .....	2-54
<b>Chapter 3</b>		
Table 3-1	Glazing Protection Levels Based on Fragment Impact Locations .....	3-21
Table 3-2	Correlation of GSA Glazing Performance Conditions and DoD Levels of Protection for New Buildings .....	3-22
<b>Chapter 4</b>		
Table 4-1	DoD Minimum Antiterrorism (AT) Standards for New Buildings .....	4-9
Table 4-2	Correlation of DoD Level of Protection to Incident Pressure .....	4-10
Table 4-3	Damage Approximations .....	4-19
<b>Chapter 5</b>		
Table 5-1	Comparison of ASHRAE Standards 52.1 and 52.2.....	5-12
Table 5-2	Indicators of a Possible Chemical Incident.....	5-34
Table 5-3	Indicators of a Possible Biological Incident.....	5-35
Table 5-4	Indicators of a Possible Radiological Incident.....	5-36

## FIGURES

### Chapter 1

Figure 1-1	Recent acts of terrorism.....	1-2
Figure 1-2	Total facilities struck by international terrorist attacks in 1997-2002 and total facilities attacked in 2002 .....	1-3
Figure 1-3	The assessment process model.....	1-5
Figure 1-4	Satellite imagery/GIS tool.....	1-7
Figure 1-5	Satellite imagery/GIS tool.....	1-8
Figure 1-6	Aggressor weapons .....	1-15
Figure 1-7	Estimated plume from a 1-ton chlorine spill in Washington, DC .....	1-16
Figure 1-8	Facility system interactions .....	1-23
Figure 1-9	Common system vulnerabilities .....	1-35
Figure 1-10	Non-redundant critical functions collocated near loading dock .....	1-41
Figure 1-11	Vulnerability examples.....	1-42
Figure 1-12	Typical building design and construction process .....	1-43
Figure 1-13	Risk management choices .....	1-44

### Chapter 2

Figure 2-1	An example of using GIS to identify adjacent hazards .....	2-5
Figure 2-2	Clustered versus dispersed site layouts .....	2-8
Figure 2-3	Clustering to enhance surveillance opportunities while minimizing views into the buildings .....	2-8
Figure 2-4	Streetscape security elements.....	2-17
Figure 2-5	Blocking of sight lines .....	2-20

Figure 2-6	Improper building siting and view relationships .....	2-21
Figure 2-7	Clear zone with unobstructed views.....	2-21
Figure 2-8	Concept of stand-off distance .....	2-22
Figure 2-9	Stand-off distance and building separation.....	2-23
Figure 2-10	Exclusive and non-exclusive zones.....	2-26
Figure 2-11	Application of perimeter barrier elements .....	2-28
Figure 2-12	Using street closing to create a controlled access area.....	2-31
Figure 2-13	Sample bollard applications .....	2-33
Figure 2-14	Examples of active and passive vehicle barriers .....	2-35
Figure 2-15	Combined multi-user gate .....	2-37
Figure 2-16	Summary of site mitigation measures .....	2-53

### **Chapter 3**

Figure 3-1	Glazed areas perpendicularly oriented away from streets .....	3-5
Figure 3-2	Re-entrant corners in a floor plan .....	3-6
Figure 3-3	Offset doors through foyer .....	3-7
Figure 3-4	Side view of a test structure illustrating performance conditions of Table 3-2.....	3-22
Figure 3-5	An unprotected window subject to a large explosion .....	3-23
Figure 3-6	Narrow and recessed windows with sloped sills.....	3-29
Figure 3-7	Sacrificial roof.....	3-33
Figure 3-8	Example of protecting outdoor air intakes .....	3-36
Figure 3-9	Example of elevated air intake .....	3-36



Figure 3-10 Another example of protecting outdoor air intakes.....	3-37
---	------

Figure 3-11 Example of enclosing an existing vulnerable air intake .....	3-38
---	------

Figure 3-12 Physical security devices.....	3-48
--	------

## **Chapter 4**

Figure 4-1 Typical pressure-time history .....	4-2
--	-----

Figure 4-2 Reflected pressure coefficient vs. angle of incidence .....	4-3
---	-----

Figure 4-3 Typical impulse waveform.....	4-4
--	-----

Figure 4-4 Blast pressure effects on a structure.....	4-7
---	-----

Figure 4-5 Explosives environments - blast range to effects .....	4-11
--	------

Figure 4-6 Blast analysis of a building for a typical car bomb detonated in the building's parking lot.....	4-12
--	------

Figure 4-7 Blast analysis of a building for a typical large truck bomb detonated in the building's parking lot.....	4-12
---	------

Figure 4-8 Relationship of cost to stand-off distance .....	4-13
---	------

Figure 4-9 Stand-off distance and its relationship to blast impact as modeled on the Khobar Towers site .....	4-15
---	------

Figure 4-10 Incident overpressure measured in pounds per square inch, as a function of stand-off distance and net explosive weight (pounds-TNT) .....	4-17
--	------

## **Chapter 5**

Figure 5-1 Universal-fit escape hood.....	5-6
---	-----

Figure 5-2 Scanning electron microscope image of a polyester-glass fiber filter .....	5-8
--	-----

Figure 5-3	Four primary filter collection mechanisms .....	5-9
Figure 5-4	Classic collection efficiency curve .....	5-10
Figure 5-5	A bag filter and HEPA filter.....	5-12
Figure 5-6	Comparison of filter collection efficiency based on particle size .....	5-13
Figure 5-7	Typical performance of a HEPA 99.97% .....	5-14
Figure 5-8	Scanning electron microscope image of activated carbon pores .....	5-14
Figure 5-9	Charcoal filter beds.....	5-17
Figure 5-10	UVGI array used for air disinfection with reflective surfaces .....	5-19
Figure 5-11	A military FFA 580 air filtration system containing both a HEPA filter and an ASZM-TEDA carbon adsorber as part of an overpressure system .....	5-21
Figure 5-12	A commercial air filtration unit .....	5-22
Figure 5-13	An IMS chemical detector designed for installation in HVAC systems .....	5-29
Figure 5-14	Placards associated with chemical incidents.....	5-35
Figure 5-15	Placards associated with biological incidents.....	5-36
Figure 5-16	Placards associated with radiological incidents.....	5-36

**M**itigating the threat of terrorist attacks against high occupancy buildings is a challenging task. It is difficult to predict how, why, and when terrorists may attack. Many factors must be considered in creating a safe building environment. This chapter presents several methodologies for architects and engineers to quantify risk and to identify the most effective mitigation measures to achieve a desired level of protection against terrorist attacks at an acceptable cost. The methodologies presented herein can be used for new buildings during the design process, as well as for existing buildings undergoing renovation. Sections 1.1 to 1.5 will discuss the assessment process, asset value assessment, threat/hazard assessment, vulnerability assessment, risk assessment, and risk management to help architects and engineers identify the best and most cost-effective terrorism mitigation measures for each building's unique security needs. Section 1.6 presents the Building Vulnerability Assessment Checklist to support the assessment process.

One of the primary objectives of this manual is to establish a common framework of terminology and the transfer of design concepts that have been in use by the United States (U.S.) Department of Defense (DoD), military services, the Department of State (DOS), and the General Services Administration (GSA) to commercial practice. The beginning point is to establish a basis for design by identifying the threat or hazard to be designed against. Within the military services, intelligence community, and law enforcement, the term “threat” is typically used to describe the design criteria for terrorism or manmade disasters. Within the Federal Emergency Management Agency (FEMA) and other civil agencies, the term “hazard” is used in several different contexts. “Natural hazard” typically refers to a natural event such as a flood, wind, or seismic disaster. “Human-caused (or manmade) hazards” are “technological hazards” and “terrorism.” These are distinct from natural hazards primarily in that they originate from human activity. Furthermore, “technological hazards” are generally

assumed to be accidental and that their consequences are unintended. For the sake of simplicity, this manual will use the terms “threat” and “hazard” when referring to terrorism and manmade disasters, respectively.

Terrorism and physical attacks on buildings have continued to increase in the past decade. The geographical isolation of the United States is not a sufficient barrier to prevent an attack on U.S. cities and citizens. Figures 1-1 and 1-2 demonstrate the far-reaching incidents and diverse natures and targets of recent terrorist attacks.

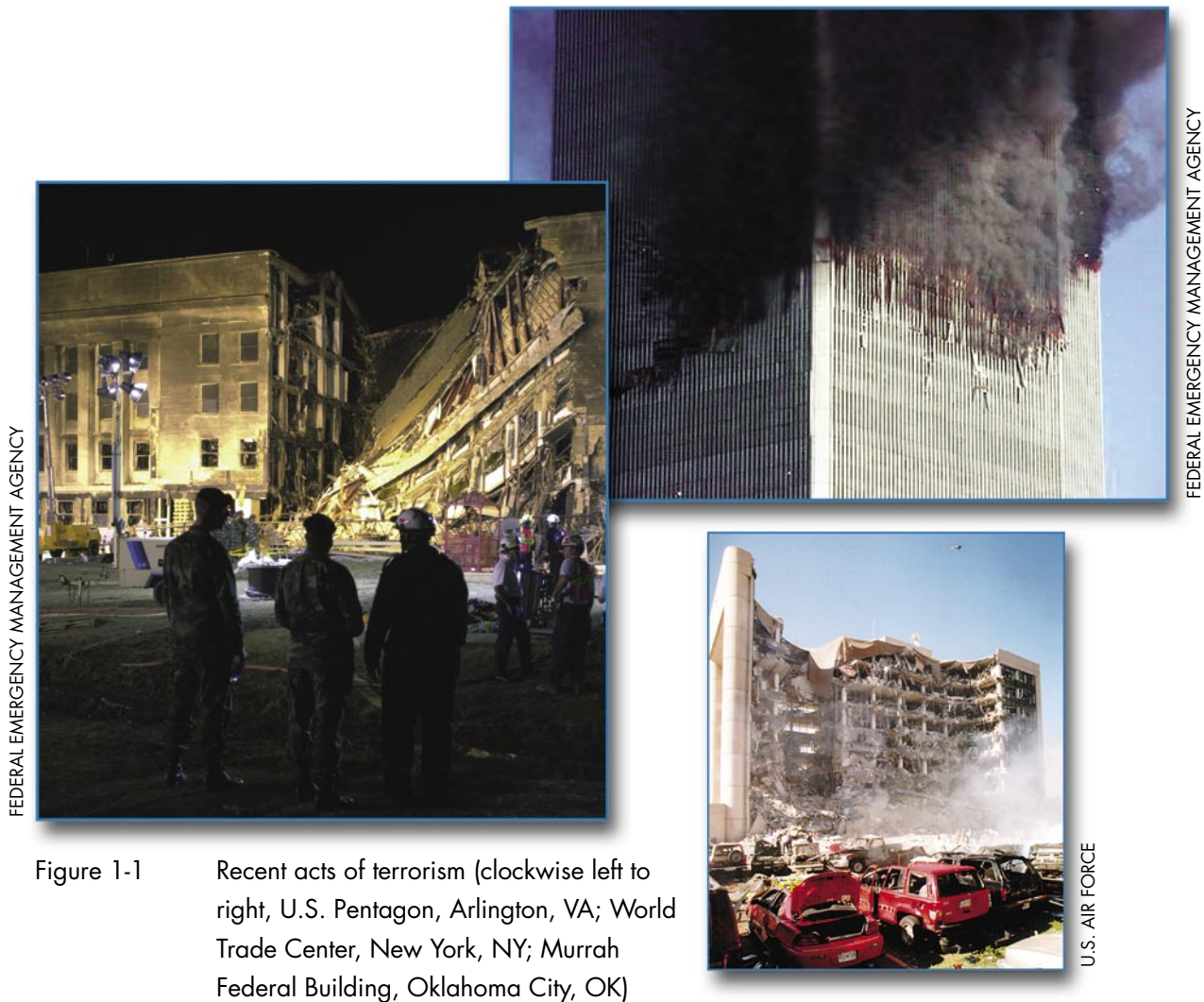


Figure 1-1 Recent acts of terrorism (clockwise left to right, U.S. Pentagon, Arlington, VA; World Trade Center, New York, NY; Murrah Federal Building, Oklahoma City, OK)

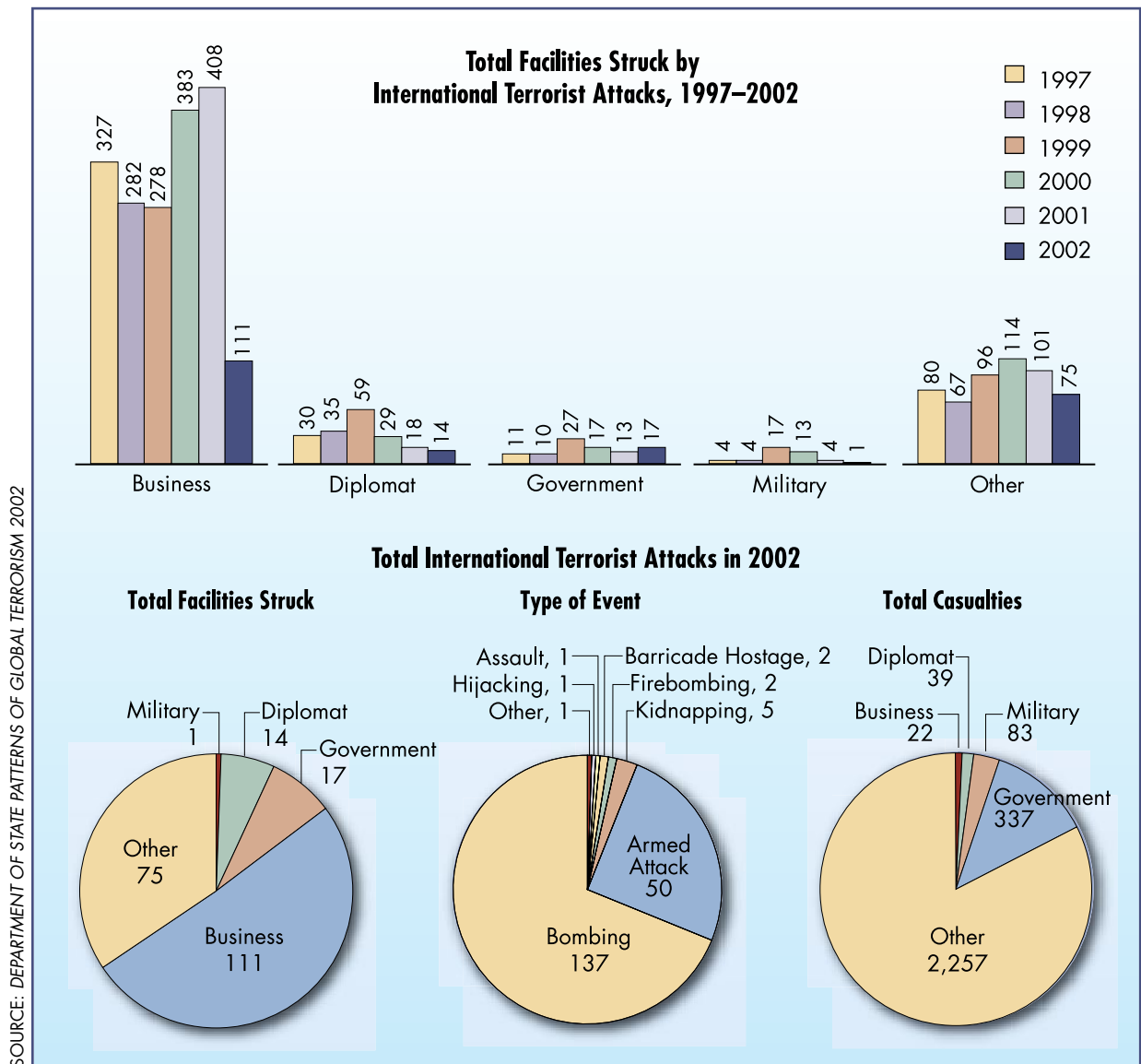


Figure 1-2 Total facilities struck by international terrorist attacks in 1997-2002 and total facilities attacked in 2002

Design of buildings to survive natural hazards is a concept that is well understood by the design community. Many years of historical and quantitative data, and probabilities associated with the cycle, duration, and magnitude of natural hazards exist. Conversely, design of buildings that can survive the threat and impact of a terrorist attack is based on qualitative factors that evaluate organization requirements, recovery efforts and impacts, and loss

of personnel and infrastructure, but have no predictable period of recurrence or damage probability. Terrorist attacks are often categorized as low probability, but potentially high consequence, events. Building designs must include physical security measures as an integral part of the design process.

This chapter presents selected methodologies to determine asset value, analyze the threat/hazard, and evaluate vulnerabilities to complete the risk assessment. These elements of information become the input for determining relative levels of risk. Higher risk hazards may require more complex mitigation measures to reduce risk. Mitigation measures are conceived by the design professional and are best incorporated into the building architecture, building systems, and operational parameters, with consideration for life-cycle costs.

In order to create a safe environment, many factors must be considered. Figure 1-3 depicts the assessment process presented in this document to help identify the best and most cost-effective terrorism mitigation measures for a building's own unique security needs. The first part of the assessment process identifies the value of a building's assets (described in Section 1.1) that need to be protected. The second step is to conduct a threat assessment wherein the threat or hazard is identified, defined, and quantified (see Section 1.2). For terrorism, the threat is the aggressors (people or groups) that are known to exist and that have the capability and a history of using hostile actions, or that have expressed intentions for using hostile actions against potential targets, as well as on whom there is current credible information on targeting activity (surveillance of potential targets) or indications of preparation for terrorist acts. The capabilities and histories of the aggressors include the tactics they have used to achieve their ends.

After conducting a threat assessment, the next step is to conduct a vulnerability assessment (see Section 1.3). A vulnerability assessment evaluates the potential vulnerability of the critical assets against a broad range of identified threats/hazards. In and of itself, the vulnerability assessment provides a basis for determining mitigation

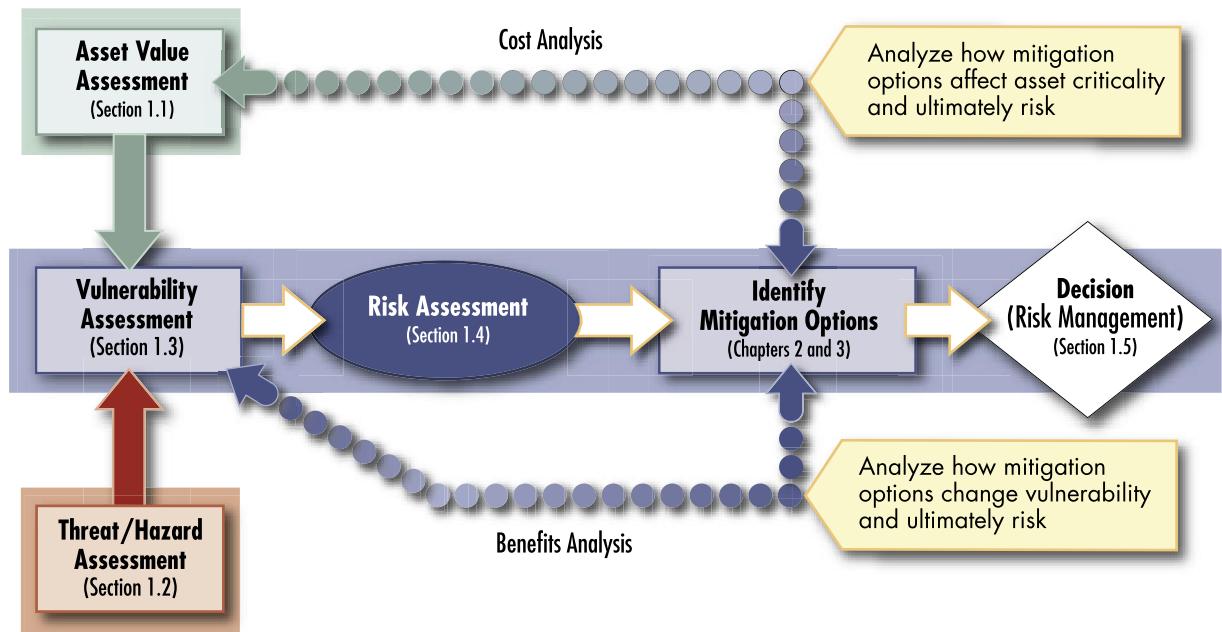


Figure 1-3 The assessment process model

measures for protection of the critical assets. The vulnerability assessment is the bridge in the methodology between threat/hazard, asset value, and the resultant level of risk.

The next step of the process is the risk assessment (see Section 1.4). The risk assessment analyzes the threat, asset value, and vulnerability to ascertain the level of risk for each critical asset against each applicable threat. Inherent in this is the likelihood or probability of the threat occurring and the consequences of the occurrence. Thus, a very high likelihood of occurrence with very small consequences may require simple low cost mitigation measures, but a very low likelihood of occurrence with very grave consequences may require more costly and complex mitigation measures. The risk assessment should provide a relative risk profile. High-risk combinations of assets against associated threats, with identified vulnerability, allow prioritization of resources to implement mitigation measures.

When starting the design process for any new building or the renovation of an existing one, various owner, statutory, and building



use inputs are required. These inputs must be integrated to ensure that mandatory building code requirements are met, the building will meet the owner's functional needs, and natural and manmade hazards are mitigated to an acceptable level. In some cases, mitigation measures to enhance security may be in conflict with other design intentions. The assessment process helps to ensure an understanding of risk, so that it can be consciously addressed within the design process with available resources.

For natural hazards (earthquakes, grassland and forest fires, floods, and winds) and building fire hazards (technological accidents), information is available in building codes, industry standards, and FEMA guidelines. For manmade hazards, the suggested course of action is less well defined. The United States has not yet developed building standards similar to those of the United Kingdom, which has a greater history of contending with repeated terrorism on its home soil. Helpful information may be found in a strategic plan or a site master plan, or it may have to be developed during initial design through interviews with building owners, staff, occupants, utility companies, local law enforcement, and others.

There are many tools and techniques available to the designer for the development of new building designs, the renovation of existing buildings, and mitigation of vulnerabilities. Advances in commercial satellite imagery, Geographic Information Systems (GIS) (see Figures 1-4 and 1-5), structural hardening, glass fragmentation films, physical security systems, and many other building related technologies provide the design professional with numerous tools to design buildings to better protect occupants from terrorist acts.

Another challenge for the design team is to present appropriate information to the building owner/decision-maker in a manner that allows him or her to make a rational, informed decision. Ideally, design basis threats will be identified and agreed upon at the earliest stages of design (no later than preliminary design). The reason for this is twofold. First, the designer must have a known



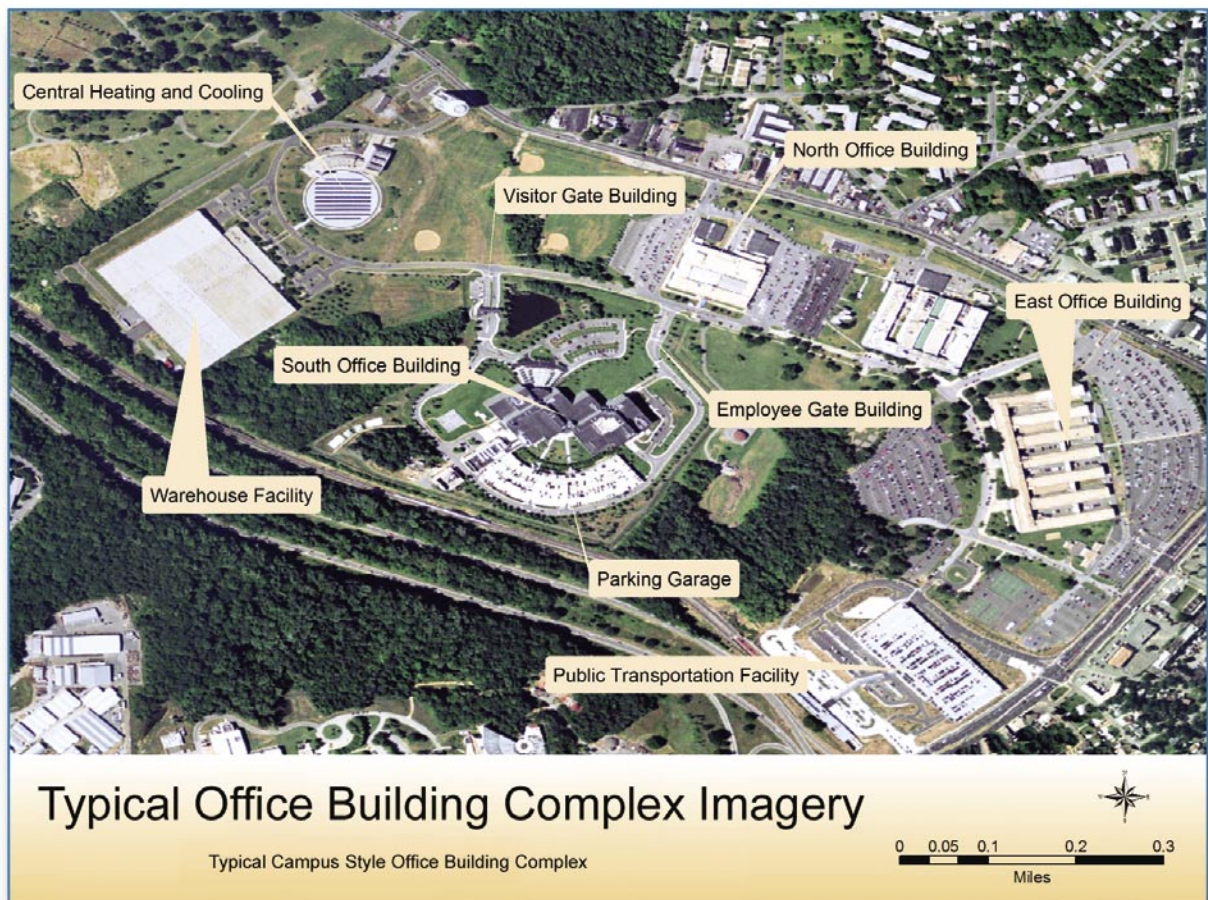


Figure 1-4 Satellite imagery/GIS tool

quantity against which to design. Second, by considering all threats/hazards (especially manmade threats) early in the design, there are potential synergies among mitigating actions. One mitigation strategy can be beneficial against more than one hazard for little difference in cost. As an example, designing moment frame connections between floors and columns and reinforcing exterior walls can mitigate against winds, explosive blasts, and earthquakes. Thus, in order to design mitigation measures for manmade hazards, the designer must have some appreciation of the assessment of threat/hazard, asset value, vulnerability, and risk to assist the building owner/decision-maker.

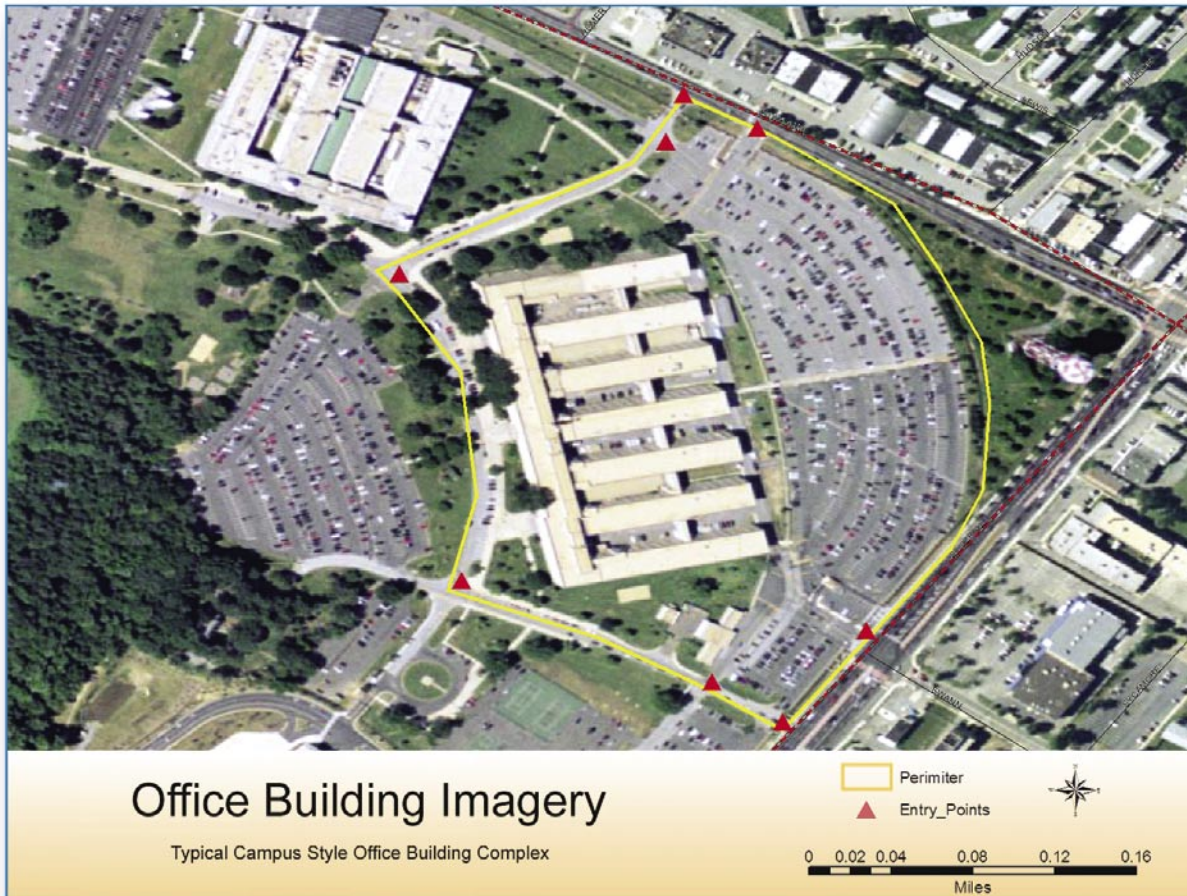


Figure 1-5 Satellite imagery/GIS tool

Based on the methodologies discussed in this chapter, the assessment process follows a logical flow:

- **Asset Value**
  - Identify criticality of assets
  - Identify number of people in a building
- **Threat/Hazard Assessment**
  - Identify each threat/hazard
  - Define each threat/hazard
  - Determine threat level for each threat/hazard
- **Vulnerability Assessment**
  - Identify site and building systems design issues



- Evaluate design issues against type and level of threat
- Determine level of protection sought for each mitigation measure against each threat

#### ○ Risk Assessment

- Likelihood of occurrence
- Impact of occurrence (loss of life, property, and function)
- Determine relative risk for each threat against each asset
- Select mitigation measures that have the greatest benefit/cost for reducing risk

The goal of the assessment process is to achieve the level of protection sought through implementation of mitigation measures in the building design. These measures may reduce risk by deterring, detecting, denying, or devaluing the potential threat element prior to or during execution of an enemy attack. Mitigation measures may also reduce risk of damage or injury by providing an acceptable level of protection if the hazard does occur, which may also serve to further deter an aggressor. For example, the Murrah Federal Building in Oklahoma City became the target of an aggressor when he was deterred from attacking his primary target, the Federal Bureau of Investigation (FBI) building, because it was too difficult to get the attack vehicle close to the FBI building. He was able to park immediately adjacent to the Murrah Federal Building and successfully target the office of the Bureau of Alcohol, Tobacco, and Firearms (ATF), which was located in the Murrah Federal Building.

The remainder of this chapter describes the general concepts of asset value, threat/hazard, vulnerability, and risk assessments for manmade disasters and presents several methodologies and techniques that can be used by an organization in conducting these assessments.

**Deter:** The process of making the target inaccessible or difficult to defeat with the weapon or tactic selected. It is usually accomplished at the site perimeter using highly visible electronic security systems, fencing, barriers, lighting and security personnel; and in the building by securing access with locks and electronic monitoring devices.

**Detect:** The process of using intelligence sharing and security services response to monitor and identify the threat before it penetrates the site perimeter or building access points.

**Deny:** The process of minimizing or delaying the degree of site or building infrastructure damage or loss of life or protecting assets by designing or using infrastructure and equipment designed to withstand blast and chemical, biological, or radiological effects.

**Devalue:** The process of making the site or building of little to no value or consequence, from the terrorists' perspective, such that an attack on the facility would not yield their desired result.

## 1.1 ASSET VALUE ASSESSMENT

This section will describe how to perform an asset value assessment (the first step of the assessment process), to identify people and the asset value. To facilitate identifying people and the value of a building's assets, it is useful to conduct interviews of the people who are most familiar with them. Inputs from building owners, facility staff, and tenants, as well as any others who can help identify the most valuable assets, should be sought. In order to conduct productive interviews, a list of areas to be covered should be generated and prioritized prior to the actual interviews. Thorough planning and research to generate relevant questions will aid the process and yield better results.

An asset is a resource of value requiring protection.<sup>1</sup> An asset can be tangible (e.g., tenants, buildings, facilities, equipment, activities, operations, and information) or intangible (e.g., processes or a company's reputation). In order to achieve the greatest risk reduction at the least cost, identifying and prioritizing a building's critical assets is a vital first step in the process to identify the best mitigation measures to improve its level of protection prior to a terrorist attack. Recognizing that people are a building's most critical asset, the process described below will help identify and prioritize infrastructure where people are most at risk and require protection.

Identifying a building's critical assets is accomplished in a two-step process:

**Step 1:** Define and understand the building's core functions and processes

**Step 2:** Identify building infrastructure

- Critical components/assets
- Critical information systems and data
- Life safety systems and safe haven areas
- Security systems

<sup>1</sup> Appendix B is a glossary of assessment and security terminology. Appendix C contains chemical, biological, and radiological terms.

### **1.1.1 Identifying Building Core Functions**

The initial step of an asset value assessment is the determination of core functions and processes necessary for the building to continue to operate or provide services after an attack. The reason for identifying core functions/processes is to focus the design team on what a building does, how it does it, and how various threats can affect the building. This provides more discussion and results in a better understanding of asset value. Factors that should be considered include:

- What are the building's primary services or outputs?
- What critical activities take place at the building?
- Who are the building's occupants and visitors?
- What inputs from external organizations are required for a building's success?

### **1.1.2 Identifying Building Infrastructure**

After the core functions and processes are identified, an evaluation of building infrastructure is the next step. To help identify and value rank infrastructure, the following should be considered, keeping in mind that the most vital asset for every building is its people:

- Identify how many people may be injured or killed during a terrorist attack that directly affects the infrastructure.
- Identify what happens to building functions, services, or occupant satisfaction if a specific asset is lost or degraded. (Can primary services continue?)
- Determine the impact on other organizational assets if the component is lost or can not function.
- Determine if critical or sensitive information is stored or handled at the building.
- Determine if backups exist for the building's assets.
- Determine the availability of replacements.

- Determine the potential for injuries or deaths from any catastrophic event at the building's assets.
- Identify any critical building personnel whose loss would degrade, or seriously complicate the safety of building occupants during an emergency.
- Determine if the building's assets can be replaced and identify replacement costs if the building is lost.
- Identify the locations of key equipment.
- Determine the locations of personnel work areas and systems.
- Identify the locations of any personnel operating "outside" a building's controlled areas.
- Determine, in detail, the physical locations of critical support architectures:
  - Communications and information technology (IT - the flow of critical information)
  - Utilities (e.g., facility power, water, air conditioning, etc.)
  - Lines of communication that provide access to external resources and provide movement of people (e.g., road, rail, air transportation)
- Determine the location, availability, and readiness condition of emergency response assets, and the state of training of building staff in their use.

### **1.1.3 Quantifying Asset Value**

After a list of a building's assets or resources of value requiring protection have been identified, they should be assigned a value. Asset value is the degree of debilitating impact that would be caused by the incapacity or destruction of the building's assets. There are many scales that can be used, each with advantages and disadvantages. Because some people are used to working with linguistic scales, although many engineers and designers prefer numerical systems, this publication will use a combination of a seven-level linguistic scale and a ten-point numerical scale as

shown in Table 1-1. Obviously, the key asset for every building is its people (e.g., employees, visitors, etc.). They will always be assigned the highest asset value as in the example below.

Table 1-1: Asset Value Scale

Asset Value	
Very High	10
High	8-9
Medium High	7
Medium	5-6
Medium Low	4
Low	2-3
Very Low	1

**Very High** – Loss or damage of the building’s assets would have exceptionally grave consequences, such as extensive loss of life, widespread severe injuries, or total loss of primary services, core processes, and functions.

**High** – Loss or damage of the building’s assets would have grave consequences, such as loss of life, severe injuries, loss of primary services, or major loss of core processes and functions for an extended period of time.

**Medium High** – Loss or damage of the building’s assets would have serious consequences, such as serious injuries or impairment of core processes and functions for an extended period of time.

**Medium** – Loss or damage of the building’s assets would have moderate to serious consequences, such as injuries or impairment of core functions and processes.

**Medium Low** – Loss or damage of the building’s assets would have moderate consequences, such as minor injuries or minor impairment of core functions and processes.

**Low** – Loss or damage of the building’s assets would have minor consequences or impact, such as a slight impact on core functions and processes for a short period of time.

**Very Low** – Loss or damage of the building’s assets would have negligible consequences or impact.

**Asset Value Example.** A nominal list of assets for a typical building with assigned value is presented in Table 1-2. Please note that this is a nominal example; each building should tailor its list to its own unique situation.

Table 1-2: Nominal Building Asset Value Assessment

Asset	Value	Numeric Value
Site	Medium Low	4
Architectural	Medium	5
Structural Systems	High	8
Envelope Systems	Medium High	7
Utility Systems	Medium High	7
Mechanical Systems	Medium High	7
Plumbing and Gas Systems	Medium	5
Electrical Systems	Medium High	7
Fire Alarm Systems	High	9
IT/Communications Systems	High	8

## 1.2 THREAT/HAZARD ASSESSMENT

### 1.2.1 Threat/Hazard Identification

With any manmade hazard, it is important to understand who are the people with the intent to cause harm. For those people, it is essential to understand their weapons, tools, and tactics, realizing that weapons, tools, and tactics can change faster than a building can be modified against the threat. The threat/hazard assessment information should be sought from local law enforcement, local



emergency management, the FBI, the Centers for Disease Control and Prevention (CDC), the U.S. Department of Homeland Security (DHS), and the Homeland Security Offices (HSOs) at the state level. For technological hazards, it is also important to gather information from the local fire department and hazardous materials (HazMat) unit, Local Emergency Planning Committee (LEPC), and State Emergency Response Commission (SERC). LEPC and SERC are local and state organizations established under a U.S. Environmental Protection Agency (EPA) program. They identify critical facilities in vulnerable zones and generate emergency management plans. Additionally, most fire departments understand which industries in the local area handle the most combustible materials and the HazMat unit understands who handles materials that could have a negative impact upon people and the environment. In many jurisdictions, the HazMat unit is part of the fire department.

The aggressors (those people with intent to do harm) seek publicity for their cause, monetary gain (in some instances), or political gain through their actions. These actions injure or kill people; destroy or damage facilities, property, equipment, or resources; or steal equipment, material, or information. Their methods can be forced entry tools, vehicles, and surveillance (visual/audio; stand-off or planted). Their weapons can include incendiary devices; small arms (rifles and handguns); stand-off military-style weapons (rocket propelled grenades or mortars) (see Figure 1-6); explosives; and chemical, biological, and radiological agents (CBR, individually or combined with explosives to aid in dispersion).



Figure 1-6 Aggressor weapons

Explosives include homemade and stolen industrial and military varieties, packaged from small to very large (mail bombs to vehicle bombs). Aggressor tactics run the gamut: moving vehicle bombs; stationary vehicle bombs; exterior attacks (thrown objects like rocks, Molotov cocktails, hand grenades, or hand-placed

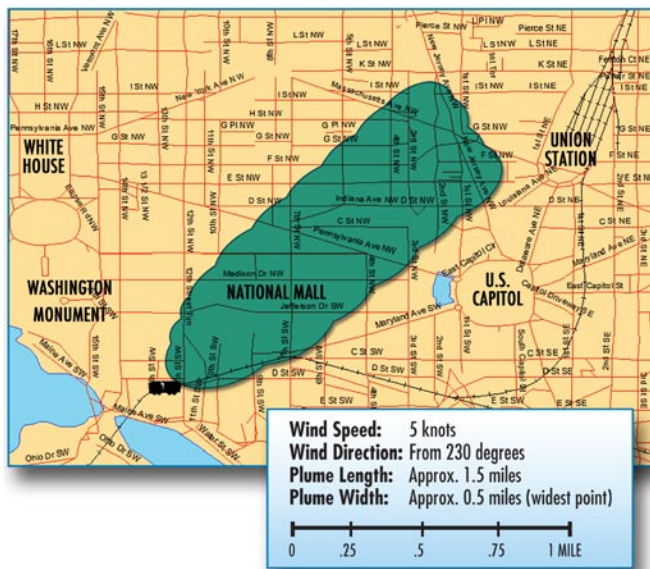


Figure 1-7 Estimated plume from a 1-ton chlorine spill in Washington, DC

bombs); stand-off weapons attacks (military or improvised larger direct and indirect fire weapons); ballistic attacks (small arms handled by one individual); covert entries (gaining entry by false credentials or circumventing security with or without weapons); mail bombs (delivered to individuals); supply bombs (larger bombs processed through shipping departments); airborne contamination (CBR agents used to contaminate the air supply of a building as notionally (hypothetically) demonstrated in Figure 1-7); and waterborne contamination (CBR agents injected into the water supply).

Table 1-3 provides insight into the various manmade hazards to consider and can be used as a tool for threat assessments. Note that Table 1-1 combines aspects of tools, weapons, explosives, and tactics. Chapters 4 and 5 provide additional information on manmade hazards, and Appendix C provides a complete list of CBR agents.

Table 1-3 provides the designer with a general profile of events associated with a spectrum of threats/hazards. The next sections will begin the process of quantifying a building's "design basis" by applying a systems engineering evaluation process to determine a building's critical functions, infrastructure, and vulnerabilities using an understanding of the aggressors, potential threat elements, a more refined definition of the threat/hazard, and methods to evaluate the risk. There are several methodologies and assessment techniques that can be used. Historically, the U.S. military methodology (with a focus on explosive effects, CBR, and personnel protection) has been used extensively for military installations and other national infrastructure assets. The DOS adopted many of the same blast and CBR design criteria, and the GSA further developed criteria for federal buildings as a result of the

attack on the Murrah Federal Building. The Department of Commerce (DOC) Critical Infrastructure Assurance Office (CIAO) established an assessment framework, which focused on information technology infrastructure.

Table 1-3: Event Profiles for Terrorism and Technological Hazards\*

Threat/Hazard	Application Mode	Duration	Extent of Effects; Static/Dynamic	Mitigating and Exacerbating Conditions
<b>Improvised Explosive Device (Bomb)</b> <ul style="list-style-type: none"> <li>- Stationary Vehicle</li> <li>- Moving Vehicle</li> <li>- Mail</li> <li>- Supply</li> <li>- Thrown</li> <li>- Placed</li> <li>- Personnel</li> </ul>	Detonation of explosive device on or near target; via person, vehicle, or projectile.	Instantaneous; additional secondary devices may be used, lengthening the duration of the threat/hazard until the attack site is determined to be clear.	Extent of damage is determined by type and quantity of explosive. Effects generally static other than cascading consequences, incremental structural failure, etc.	Blast energy at a given stand-off is inversely proportional to the cube of the distance from the device; thus, each additional increment of stand-off provides progressively more protection. Exacerbating conditions include ease of access to target; lack of barriers/shielding; poor construction; and ease of concealment of device.
<b>Chemical Agent</b> <ul style="list-style-type: none"> <li>- Blister</li> <li>- Blood</li> <li>- Choking/Lung/Pulmonary</li> <li>- Incapacitating</li> <li>- Nerve</li> <li>- Riot Control/Tear Gas</li> <li>- Vomiting</li> </ul>	Liquid/aerosol contaminants can be dispersed using sprayers or other aerosol generators; liquids vaporizing from puddles/containers; or munitions.	Chemical agents may pose viable threats for hours to weeks, depending on the agent and the conditions in which it exists.	Contamination can be carried out of the initial target area by persons, vehicles, water, and wind. Chemicals may be corrosive or otherwise damaging over time if not remediated.	Air temperature can affect evaporation of aerosols. Ground temperature affects evaporation of liquids. Humidity can enlarge aerosol particles, reducing the inhalation hazard. Precipitation can dilute and disperse agents, but can spread contamination. Wind can disperse vapors, but also cause target area to be dynamic. The micro-meteorological effects of buildings and terrain can alter travel and duration of agents. Shielding in the form of sheltering in place may protect people and property from harmful effects.

Table 1-3: Event Profiles for Terrorism and Technological Hazards\* (continued)

Threat/Hazard	Application Mode	Duration	Extent of Effects; Static/Dynamic	Mitigating and Exacerbating Conditions
<b>Arson/Incendiary Attack</b>	Initiation of fire or explosion on or near target via direct contact or remotely via projectile.	Generally minutes to hours.	Extent of damage is determined by type and quantity of device /accelerant and materials present at or near target. Effects generally static other than cascading consequences, incremental structural failure, etc.	Mitigation factors include built-in fire detection and protection systems and fire-resistive construction techniques. Inadequate security can allow easy access to target, easy concealment of an incendiary device, and undetected initiation of a fire. Non-compliance with fire and building codes as well as failure to maintain existing fire protection systems can substantially increase the effectiveness of a fire weapon.
<b>Armed Attack</b> - Ballistics (small arms) - Stand-off Weapons (rocket propelled grenades, mortars)	Tactical assault or sniper attacks from a remote location.	Generally minutes to days.	Varies, based upon the perpetrator's intent and capabilities.	Inadequate security can allow easy access to target, easy concealment of weapons, and undetected initiation of an attack.
<b>Biological Agent</b> - Anthrax - Botulism - Brucellosis - Plague - Smallpox - Tularemia - Viral Hemorrhagic Fevers - Toxins (Botulinum, Ricin, Staphylococcal Enterotoxin B, T-2 Mycotoxins)	Liquid or solid contaminants can be dispersed using sprayers/aerosol generators or by point or line sources such as munitions, covert deposits, and moving sprayers. May be directed at food or water supplies.	Biological agents may pose viable threats for hours to years, depending on the agent and the conditions in which it exists.	Depending on the agent used and the effectiveness with which it is deployed, contamination can be spread via wind and water. Infection can be spread via human or animal vectors.	Altitude of release above ground can affect dispersion; sunlight is destructive to many bacteria and viruses; light to moderate winds will disperse agents, but higher winds can break up aerosol clouds; the micro-meteorological effects of buildings and terrain can influence aerosolization and travel of agents.

Table 1-3: Event Profiles for Terrorism and Technological Hazards\* (continued)

Threat/Hazard	Application Mode	Duration	Extent of Effects; Static/Dynamic	Mitigating and Exacerbating Conditions
<b>Cyberterrorism</b>	Electronic attack using one computer system against another.	Minutes to days.	Generally no direct effects on built environment.	Inadequate security can facilitate access to critical computer systems, allowing them to be used to conduct attacks.
<b>Agriterrorism</b>	Direct, generally covert contamination of food supplies or introduction of pests and/or disease agents to crops and livestock.	Days to months.	Varies by type of incident. Food contamination events may be limited to discrete distribution sites, whereas pests and diseases may spread widely. Generally no effects on built environment.	Inadequate security can facilitate adulteration of food and introduction of pests and disease agents to crops and livestock.
<b>Radiological Agent</b> - Alpha - Beta - Gamma	Radioactive contaminants can be dispersed using sprayers/aerosol generators, or by point or line sources such as munitions, covert deposits, and moving sprayers.	Contaminants may remain hazardous for seconds to years, depending on material used.	Initial effects will be localized to site of attack; depending on meteorological conditions, subsequent behavior of radioactive contaminants may be dynamic.	Duration of exposure, distance from source of radiation, and the amount of shielding between source and target determine exposure to radiation.
<b>Nuclear Device</b>	Detonation of nuclear device underground, at the surface, in the air or at high altitude.	Light/heat flash and blast/shock wave last for seconds; nuclear radiation and fallout hazards can persist for years.  Electromagnetic pulse from a high-altitude detonation lasts for seconds and affects unprotected electronic systems.	Initial light, heat, and blast effects of a subsurface, ground, or air burst are static and are determined by the device's characteristics and employment; fallout of radioactive contaminants may be dynamic, depending on meteorological conditions.	Harmful effects of radiation can be reduced by minimizing the time of exposure. Light, heat, and blast energy decrease logarithmically as a function of distance from seat of blast. Terrain, forestation, structures, etc., can provide shielding by absorbing and/or deflecting blast, radiation, and radioactive contaminants.

Table 1-3: Event Profiles for Terrorism and Technological Hazards\* (continued)

Threat/Hazard	Application Mode	Duration	Extent of Effects; Static/Dynamic	Mitigating and Exacerbating Conditions
<b>Hazardous Material Release</b> <b>(fixed site or transportation)</b> <ul style="list-style-type: none"> <li>- Toxic Industrial Chemicals and Materials (Organic vapors: cyclohexane; Acid gases: cyanogens, chlorine, hydrogen sulfide; Base gases: ammonia; Special cases: phosgene, formaldehyde)</li> </ul>	Solid, liquid, and/or gaseous contaminants may be released from fixed or mobile containers.	Hours to days.	Chemicals may be corrosive or otherwise damaging over time. Explosion and/or fire may be subsequent. Contamination may be carried out of the incident area by persons, vehicles, water, and wind.	As with chemical weapons, weather conditions will directly affect how the hazard develops. The micro-meteorological effects of buildings and terrain can alter travel and duration of agents. Shielding in the form of sheltering in place may protect people and property from harmful effects. Non-compliance with fire and building codes as well as failure to maintain existing fire protection and containment features can substantially increase the damage from a hazardous materials release.
<b>Unauthorized Entry</b> <ul style="list-style-type: none"> <li>- Forced</li> <li>- Covert</li> </ul>	Use of hand or power tools, weapons, or explosives to create a man-sized opening or operate an assembly (such as a locked door), or use of false credentials to enter a building.	Minutes to hours, depending upon the intent.	If goal is to steal or destroy physical assets or compromise information, the initial effects are quick, but damage may be long lasting. If intent is to disrupt operations or take hostages, the effects may last for a long time, especially if injury or death occurs.	Standard physical security building design should be the minimum mitigation measure. For more critical assets, additional measures, like closed circuit television or traffic flow that channels visitors past access control, aids in detection of this hazard.

Table 1-3: Event Profiles for Terrorism and Technological Hazards\* (continued)

Threat/Hazard	Application Mode	Duration	Extent of Effects; Static/Dynamic	Mitigating and Exacerbating Conditions
<b>Surveillance</b> <ul style="list-style-type: none"> <li>- Acoustic</li> <li>- Electronic eavesdropping</li> <li>- Visual</li> </ul>	Stand-off collection of visual information using cameras or high powered optics, acoustic information using directional microphones and lasers, and electronic information from computers, cell phones, and hand-held radios. Placed collection by putting a device "bug" at the point of use.	Usually months.	This is usually the prelude to the loss of an asset. A terrorist surveillance team spends much time looking for vulnerabilities and tactics that will be successful. This is the time period that provides the best assessment of threat because it indicates targeting of the building.	Building design, especially blocking lines of sight and ensuring the exterior walls and windows do not allow sound transmission or acoustic collection, can mitigate this hazard.

\* SOURCE: FEMA 386-7, *INTEGRATING HUMAN-CAUSED HAZARDS INTO MITIGATION PLANNING*, SEPTEMBER 2002

### 1.2.2 Threat Definition of Physical Attack on a Building

To stop a terrorist or physical attack on a building is very difficult; any building or site can be breached or destroyed. However, the more secure the building or site and the better the building is designed to withstand an attack, the better the odds the building will not be attacked or, if attacked, will suffer less damage. Terrorists generally select targets that have some value as a target, such as an iconic commercial property, symbolic government building, or structure likely to inflict significant emotional or economic damage such as a shopping mall or major seaport. A manmade threat/hazard analysis requires interface with security and intelligence organizations that understand the locality, the region, and the nation. These organizations include the police department (whose jurisdiction includes the building or site), the local state police office, and the local office of the FBI. In many areas of the country, there are threat coordinating committees, including FBI Joint Terrorism Task Forces, that facilitate the sharing of informa-

tion. A common method to evaluate terrorist threats is to analyze five factors: existence, capability, history, intention, and targeting.

**Existence** addresses the questions: Who is hostile to the assets, organization, or community of concern? Are they present or thought to be present? Are they able to enter the country or are they readily identifiable in a local community upon arrival?

**Capability** addresses the questions: What weapons have been used in carrying out past attacks? Do the aggressors need to bring them into the area or are they available locally?

**History** addresses the questions: What has the potential threat element done in the past and how many times? When was the most recent incident and where, and against what target? What tactics did they use? Are they supported by another group or individuals? How did they acquire their demonstrated capability?

**Intention** addresses the questions: What does the potential threat element or aggressor hope to achieve? How do we know this (e.g., published in books or news accounts, speeches, letters to the editor, informant)?

**Targeting** addresses the questions: Do we know if an aggressor (we may not know which specific one) is performing surveillance on our building, nearby buildings, or buildings that have much in common with our organization? Is this information current and credible, and indicative of preparations for terrorist operations (manmade hazards)?

The threat/hazard analysis for any building can range from a general threat/hazard scenario to a very detailed examination of specific groups, individuals, and tactics that the building may need to be designed to repel or defend against.

A terrorist or aggressor will analyze the building or target as shown in Figure 1-8 to determine the type of attack, type of weapon, and tactics to employ to defeat the building or critical mission/business function.



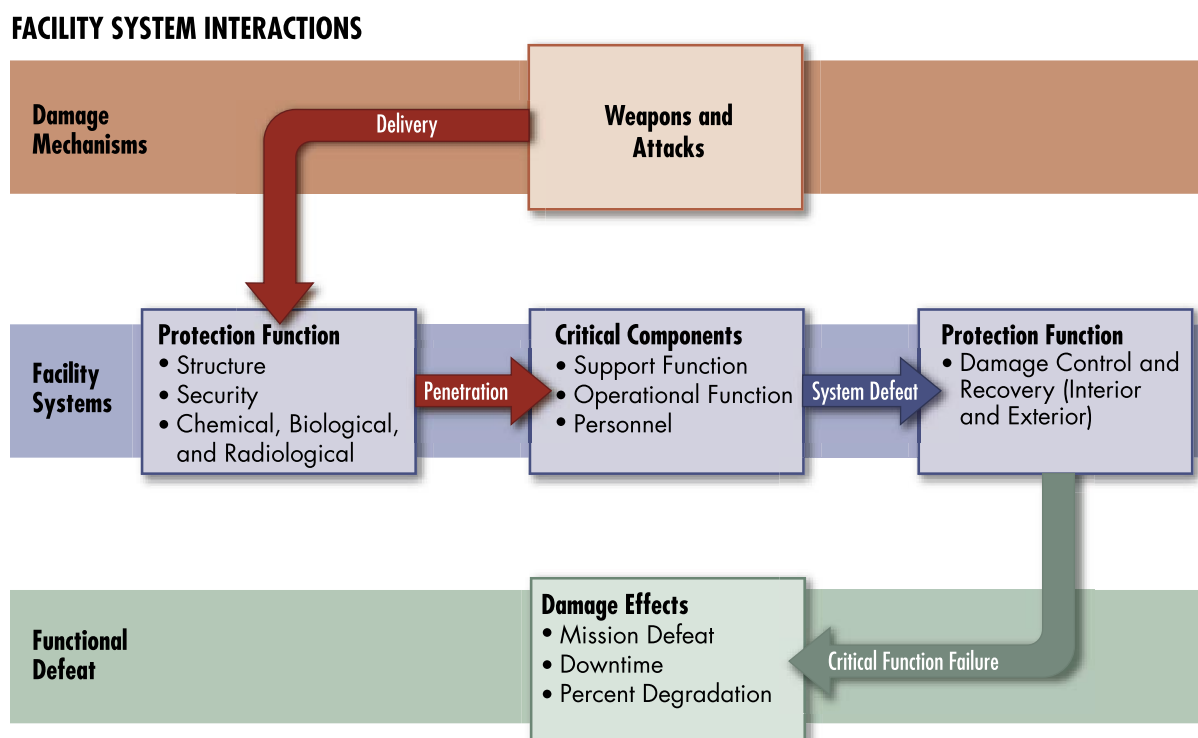


Figure 1-8 Facility system interactions

The Homeland Security Advisory System has five threat levels that provide a general indication of risk of terrorist attack. In Table 1-4, the five factors commonly used to evaluate terrorist threats have been layered onto the Homeland Security Advisory levels. If the anticipated threat or projected use of the building warrants it, a detailed threat analysis should be developed in coordination with local law enforcement, intelligence, and civil authorities in order to more quantitatively determine the vulnerability or risk. Having conducted a threat analysis and having a good conceptual idea of the preliminary building design and site layout, the next step is to conduct a vulnerability assessment to identify weaknesses that can be exploited by an aggressor and to help identify specific design features and establish operational parameters to mitigate them.

Table 1-4: Homeland Security Threat Conditions

Threat Level	Threat Analysis Factors				
	Existence	Capability	History	Intentions	Targeting
Severe (Red)	●	●	●	●	●
High (Orange)	●	●	●	●	□
Elevated (Yellow)	●	●	●	□	
Guarded (Blue)	●	●	□		
Low (Green)	●	□			

● Factor must be present      □ Factor may or may not be present

Please note the DHS does not use these threat analysis factors to determine threat level.

SOURCE: COMMONWEALTH OF KENTUCKY OFFICE OF HOMELAND SECURITY

### 1.3 VULNERABILITY ASSESSMENT

Knowing the expected threat/hazard capability allows the designer to integrate the threat knowledge with specific building and site information by conducting a vulnerability assessment. A vulnerability assessment is an in-depth analysis of the building functions, systems, and site characteristics to identify building weaknesses and lack of redundancy, and determine mitigations or corrective actions that can be designed or implemented to reduce the vulnerabilities. A vulnerability assessment should be performed for existing buildings and the process incorporated into the design for new construction and renovation.

Table 1-5 contains vulnerability and consequence aspects and provides an objective approach to determine a relative value of vulnerability for the building or site. An alternate method for determining a relative value is presented in Table 1-6, from the U.S. Department of Justice (DOJ), as applicable to GSA buildings. This method provides a suggestion of “security measures” for typical sizes and types of sites, in addition to a transferable example of appropriate security measures for typical locations and occupancies. Tables 1-5 and 1-6 address operational, consequential, and inherent characteristics that contribute to vul-

nerability. They are a first step and should be used in conjunction with a more detailed vulnerability assessment such as the Building Vulnerability Assessment Checklist (see Table 1-22).

Table 1-7 is an example of one approach to implement minimum building design standards to mitigate terrorist events following the methodology of Table 1-6. Note that an evaluation or vulnerability assessment still needs to be done before incorporating any mitigation measures.

Table 1-5: Site/Building Inherent Vulnerability Assessment Matrix (Partial Risk Assessment)\*

Criteria	0	1	2	3	4	5	Score
<b>Asset Visibility</b>	—	Existence not well known	—	Existence locally known	—	Existence widely known	
<b>Target Utility</b>	None	Very Low	Low	Medium	High	Very High	
<b>Asset Accessibility</b>	Remote location, secure perimeter, armed guards, tightly controlled access	Fenced, guarded, controlled access	Controlled access, protected entry	Controlled access, unprotected entry	Open access, restricted parking	Open access, unrestricted parking	
<b>Asset Mobility</b>	—	Moves or is relocated frequently	—	Moves or is relocated occasionally	—	Permanent/ fixed in place	
<b>Presence of Hazardous Materials</b>	No hazardous materials present	Limited quantities, materials in secure location	Moderate quantities, strict control features	Large quantities, some control features	Large quantities, minimal control features	Large quantities, accessible to non-staff personnel	
<b>Collateral Damage Potential</b>	No risk	Low risk/ limited to immediate area	Moderate risk/limited to immediate area	Moderate risk within 1-mile radius	High risk within 1-mile radius	High risk beyond 1-mile radius	
<b>Site Population/ Capacity</b>	0	1-250	251-500	501-1,000	1,001-5,000	> 5,000	
Total							

\* SOURCE: FEMA 386-7, *INTEGRATING HUMAN-CAUSED HAZARDS INTO MITIGATION PLANNING*, SEPTEMBER 2002

Table 1-6: Classification Table Extracts\*

Level**	Typical Location	Examples of Tenant Agencies***	Security Measures (based on evaluation)
<b>I</b>	10 Employees (Federal) 2,500 Square Feet Low Volume Public Contact Small "Store Front" Type Operation	Local Office District Office Visitor Center USDA Office Ranger Station Commercial Facilities Industrial/Manufacturing Health Care	High Security Locks Intercom Peep Hole (Wide View) Lighting w/Emergency Backup Power Controlled Utility Access Annual Employee Security Training
<b>II</b>	11 - 150 Employees (Federal) 2,500 - 80,000 Square Feet Moderate Volume Public Contact Routine Operations Similar to Private Sector and/or Facility Shared with Private Sector	Public Officials Park Headquarters Regional/State Offices Commercial Facilities Industrial Manufacturing Health Care	Entry Control Package w/Closed Circuit Television (CCTV) Visitor Control/Screening Shipping/Receiving Procedures Guard/Patrol Assessment Intrusion Detection w/Central Monitoring CCTV Surveillance (Pan-Tilt, Zoom System) Duress Alarm w/Central Monitoring
<b>III</b>	151 - 450 Employees (Federal) Multi-Story Facility 80,000 - 150,000 Square Feet Moderate/High Volume Public Contact Agency Mix: Law Enforcement Operations Court Functions Government Records	Inspectors General Criminal Investigations Regional/State Offices GSA Field Office Local Schools Commercial Facilities Industrial Manufacturing Health Care	Guard Patrol on Site Visitor Control/Screening Shipping/Receiving Procedures Intrusion Detection w/Central Monitoring CCTV Surveillance (Pan-Tilt/Zoom System) Duress Alarm w/Central Monitoring
<b>IV</b>	>450 Employees (Federal) Multi-Story Facility >150,000 Square Feet High Volume Public Contact High-Risk Law Enforcement/Intelligence Agencies District Court	Significant Buildings and Some Headquarters Federal Law Enforcement Agencies Local Schools, Universities Commercial Facilities Health Care	Extend Perimeter (Concrete/Steel Barriers) 24-Hour Guard Patrol Adjacent Parking Control Backup Power System Hardened Parking Barriers
<b>V</b>	Level IV Profile and Agency/Mission Critical to National Security	Principal Department Headquarters	Agency-Specific

\* SOURCE: U.S. DEPARTMENT OF JUSTICE, VULNERABILITY ASSESSMENT OF FEDERAL FACILITIES, JUNE 28, 1995

NOTES: \*\* ASSIGNMENT OF LEVELS TO BE BASED ON AN "ON-SITE" RISK ASSESSMENT/EVALUATION

\*\*\*EXAMPLES OF TYPICAL (BUT NOT LIMITED TO) TENANT AGENCIES FOR THIS LEVEL FACILITY

Table 1-7: Selected Extracts -- Recommended Standards Chart\*

M — Minimum Standard                      S — Standard Based On Facility Evaluation  
D — Desirable (to minimize risk)        N/A — Not Applicable

	LEVEL				
	I	II	III	IV	V
<b>PERIMETER SECURITY</b>					
<b>Parking</b>					
Control of Facility Parking	D	D	M	M	M
Control of Adjacent Parking	D	D	D	S	S
Avoid Leases Where Parking Cannot be Controlled	D	D	D	D	D
Leases Should Provide Security Control for Adjacent Parking	D	D	D	D	D
Post Signs and Arrange for Towing Unauthorized Vehicles	S	S	M	M	M
ID System and Procedures for Authorized Parking (Placard, Decal, Card Key, etc.)	D	D	M	M	M
Adequate Lighting for Parking Areas	D	D	M	M	M
<b>Closed Circuit Television (CCTV) Monitoring</b>					
CCTV Surveillance Cameras with Time Lapse Video Recording	D	S	S	M	M
Post Signs Advising of 24-Hour Video Surveillance	D	S	S	M	M
<b>Lighting</b>					
Lighting with Emergency Power Backup	M	M	M	M	M
<b>Physical Barriers</b>					
Extend Physical Perimeter with Barriers (Concrete and/or Steel Composition)	N/A	N/A	D	S	S
Parking Barriers	N/A	N/A	D	S	S
<b>ENTRY SECURITY</b>					
<b>Receiving/Shipping</b>					
Review Receiving/Shipping Procedures (Current)	M	M	M	M	M
Implement Receiving/Shipping Procedures (Modified)	D	S	M	M	M
<b>Access Control</b>					
Evaluate Facility for Security Guard Requirements	D	S	M	M	M
Security Guard Patrol	D	D	S	S	S
Intrusion Detection System with Central Monitoring Capability	D	S	M	M	M
Upgrade to Current Life Safety Standards (Fire Detection, Fire Suppression Systems, etc.)	M	M	M	M	M
<b>Entrances/Exits</b>					
X-Ray and Magnetometer at Public Entrances	N/A	D	S	S	M
Require X-Ray Screening of All Mail/Packages	N/A	D	S	M	M
Peep Holes	S	S	N/A	N/A	N/A
Intercom	S	S	N/A	N/A	N/A
Entry Control w/CCTV and Door Strikes	D	S	N/A	N/A	N/A
High Security Locks	M	M	M	M	M

Table 1-7: Selected Extracts -- Recommended Standards Chart\* (continued)

M – Minimum Standard	S – Standard Based On Facility Evaluation				
D – Desirable (to minimize risk)	N/A – Not Applicable				
	LEVEL				
	I	II	III	IV	V
INTERIOR SECURITY					
Employee/Visitor Identification					
Agency Photo ID for all Personnel Displayed at all Times	N/A	D	S	M	M
Visitor Control/Screening System	D	M	M	M	M
Visitor Identification Accountability System	N/A	D	S	M	M
Establish ID Issuing Authority	S	S	S	M	M
Utilities					
Prevent Unauthorized Access to Utility Areas	S	S	M	M	M
Provide Emergency Power to Critical Systems (Alarm Systems, Radio Communications, Computer Facilities, etc.)	M	M	M	M	M
Daycare Centers					
Evaluate Whether to Locate Daycare Facilities in Buildings with High-Threat Activities	N/A	M	M	M	M
Compare Feasibility of Locating Daycare in Facilities Outside Locations	N/A	M	M	M	M
SECURITY PLANNING					
Tenant Assignment					
Collocate Agencies with Similar Security Needs	D	D	D	D	D
Do Not Collocate High-/Low-Risk Agencies	D	D	D	D	D
Administrative Procedures					
Arrange for Employee Parking In/Near Building After Normal Work Hours	S	S	S	S	S
Conduct Background Security Checks and/or Establish Security Control Procedures for Service Contract Personnel	M	M	M	M	M
Construction/Renovation					
Install Mylar Film on all Exterior Windows (Shatter Protection)	D	D	S	M	M
Review Current Projects for Blast Standards	M	M	M	M	M
Review/Establish Uniform Standards for Construction	M	M	M	M	M
Review/Establish New Design Standard for Blast Resistance	S	S	M	M	M
Establish Street Setback for New Construction	D	D	S	M	M

\* SOURCE: EXTRACTS FROM U.S. DEPARTMENT OF JUSTICE STUDY "VULNERABILITY ASSESSMENT OF FEDERAL FACILITIES," JUNE 28, 1995

In the preceding tables, determining which “level” most nearly reflects the site and building under design or renovation may help to identify which security standards would be most appropriate to apply. The GSA method provides a more detailed analysis of a building vulnerability and good suggestions for security measures that may be appropriate to design into a building for certain occupancies and sizes of facilities. A more quantitative evaluation or ranking of one building compared to another may be required in some instances (e.g., where a building owner and designer may need to know the relative risk of one building compared to an equivalent building on another site or on the same campus).

The DOJ, Office of Justice Programs (OJP) provides an objective approach to determining vulnerability (see U.S. Department of Justice, Fiscal Year 1999 State Domestic Preparedness Equipment Program, Assessment and Strategy Development Tool Kit, May 15, 1999). DOJ’s Threat/Hazard Assessment uses seven factors that are Threat Assessment and Consequence Management oriented, and provides a quantitative means to rank buildings. It requires rating each of the seven areas and summing the ratings to determine the overall ranking for the building or site. This approach is as follows:

#### 1. Level of Visibility (Table 1-8)

What is the perceived awareness of the target’s existence and the visibility of the target to the general populace, or to the terrorist in particular?

Table 1-8: Level of Visibility

	Rating Value
Invisible – Classified location	0
Very Low Visibility – Probably not aware of existence	1
Low Visibility – Existence probably not well known	2
Medium Visibility – Existence is probably known	3
High Visibility – Existence is well known	4
Very High Visibility – Existence is obvious	5

## 2. Asset Value of Target Site (Individual Asset or Assets Accumulated within Building – Table 1-9)

What is the usefulness of the asset(s) to the population, economy, government, company, or organization? Also consider the impact on continuity of operations, hampering of emergency response, and general potential consequences. Table 1-9 could be used more than once if the value of the asset(s) impacts more than one critical area.

Table 1-9: Criticality of Target Site

	Rating Value
No Usefulness	0
Minor Usefulness	1
Moderate Usefulness	2
Significant Usefulness	3
Highly Useful	4
Critical	5

## 3. Target Value to Potential Threat Element/Aggressor (Table 1-10)

Does the target serve the ends of the aggressors identified in the Threat Assessment based on motivations (political, religious, racial, environmental, and special interests)? Table 1-10 should help to capture these motivations.

Table 1-10: Target Value to Potential Threat Element

	Rating Value
None	0
Very Low	1
Low	2
Medium	3
High	4
Very High	5

## 4. Aggressor Access to Target (Table 1-11)

Does the target have available ingress and egress for a potential aggressor?



Table 1-11: Aggressor Access to Target

	Rating Value
Fenced, Guarded, Protected Air/Consumable Entry, Controlled Access by Pass Only, No Vehicle Parking within a designated minimum distance (such as 50 feet or 80 feet)	0
Guarded, Protected Air/Consumable Entry, Controlled Access of Visitors and Non-Staff Personnel, No Vehicle Parking within the designated minimum distance	1
Protected Air/Consumable Entry, Controlled Access of Visitors and Non-Staff Personnel, No Unauthorized Vehicle Parking within the designated minimum distance	2
Controlled Access of Visitors, Unprotected Air/Consumable Entry, No Unauthorized Vehicle Parking within the designated minimum distance	3
Open Access to All Personnel, Unprotected Air/Consumable Entry, No Unauthorized Vehicle Parking within the designated minimum distance	4
Open Access to All Personnel, Unprotected Air/Consumable Entry, Vehicle Parking within the designated minimum distance	5

## 5. Target Threat of Hazard (Table 1-12)

Are CBR materials present in quantities that could become hazardous if released? These quantities could be on site or in relatively close proximity so that a theft or an accident could render them a hazard to the building or site. Take into consideration distance from building (a 1-mile radius is suggested around the building), the prevailing wind direction, the slope of the terrain, and the quantity of materials present.

Table 1-12: Target Threat of Hazard (WMD Materials)

	Rating Value
No CBR materials present	0
CBR materials present in moderate quantities, under positive control, and in secured locations	1
CBR materials present in moderate quantities and controlled	2
Major concentrations of CBR materials that have established control features and are secured in the site	3
Major concentrations of CBR materials that have moderate control features	4
Major concentrations of CBR materials that are accessible to non-staff personnel	5

## 6. Site Population Capacity (Table 1-13)

What is the maximum number of individuals at the building or site at a given time? This could be standard worst case occupancy during an average day or peak occupancy at a designated time (e.g., a movie theater).

Table 1-13: Site Population Capacity

	Rating Value
0	0
1 to 250	1
251 to 500	2
501 to 1,000	3
1,001 to 5,000	4
> 5,000	5

## 7. Potential for Collateral Damage (Mass Casualties - Table 1-14)

Address potential collateral mass casualties within a 1-mile radius of the target site. Number ranges indicate inhabitants within a 1-mile radius of the site.

Table 1-14: Potential for Collateral Damage (Mass Casualties)

	Rating Value
0-100	0
101 to 500	1
501 to 1,000	2
1,001 to 2,000	3
2,001 to 5,000	4
> 5,000	5

Each building is assessed and scored (see Table 1-15). Tables 1-15 and 1-16 contain a nominal example.

Table 1-15: Building Summary Sheet

Building/Target Name	Score
Visibility	4
Criticality	3
Value	4
Access	2
Threat of Hazard	0
Site Population	3
Collateral Mass Casualties	3
<b>Total Score</b>	<b>19</b>

The total building score can be used to rank multiple buildings (see Table 1-16) and quantitatively provides an analysis of building vulnerability from a site perspective.

Table 1-16: Building Ranking

Ranking	Building/Target Name	Total Score
1	ABC Building	23
2	DEF Building	19
3	GHI Building	14

This evaluation methodology can be applied to all building types (see Foreword). The result is independent of facility/occupancy type, except for the type of influence on population and siting.

An alternate approach is shown in Table 1-17, which uses a simplified matrix to rank the order of buildings using a numerical score of 1 (low) to 5 (high). The evaluation factors can be developed for each building use or owner-specific criteria. For Table 1-17, the factors shown illustrate a health care provider scenario:

- Criticality of Function: How critical is the building and function to the organization?

- Location: Is the building near federal buildings, major transportation, or iconic properties?
- Occupancy of Building: Are occupants mobile or non-ambulatory?
- Involvement in Community: Does the building or staff provide unique capabilities?
- Critical External Commitments: Does the building support other organizations or missions?

Table 1-17: Simplified Building Ranking Matrix

Building	Criticality of Function	Location	Occupancy of Building	Involvement in Community	Critical External Commitments	Total Score
Headquarters	2	5	3	1	4	15
Hospital 1	1	2	2	1	1	7
Hospital 2	3	2	3	4	4	16
Data Center	5	4	3	3	2	17

The objective of Tables 1-1 through 1-17 or similar assessment methodologies is to provide an analysis of a building, facility, or site and to identify the buildings that are most vulnerable from a given threat/hazard matched against specific building type or function. Having the ranked list of buildings, the next step is to conduct an in-depth vulnerability assessment of the building. The building assessment is to evaluate specific design and architectural features and identify all vulnerabilities of the building functions and building systems. Frequently, single-point-vulnerabilities exist, which are critical functions or systems that lack redundancy and, if damaged by an attack, would result in immediate organization disruption or loss of capability. These are generally the highest risk vulnerabilities. Figure 1-9 illustrates the common system vulnerabilities.

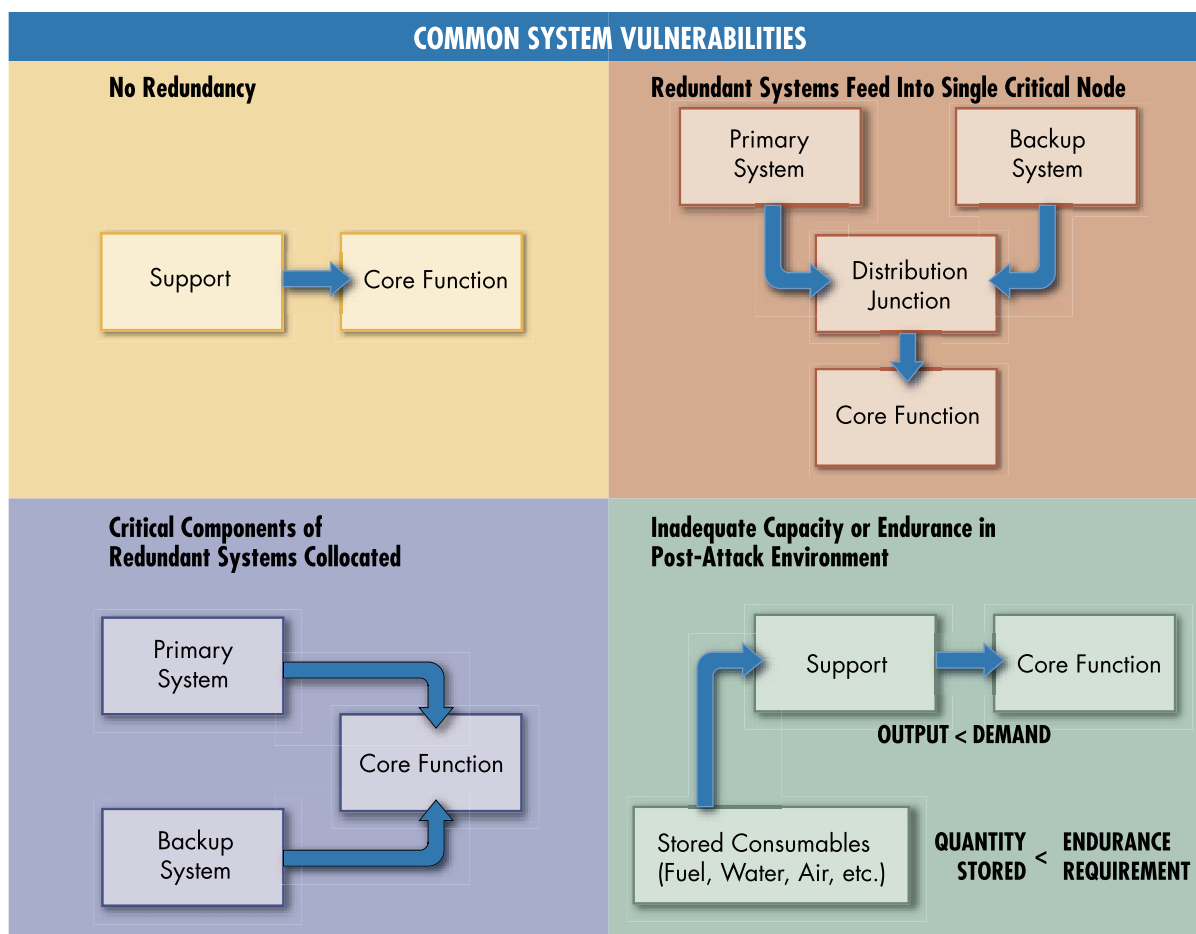


Figure 1-9 Common system vulnerabilities

## 1.4 RISK ASSESSMENT

Risk is the potential for a loss of or damage to an asset. It is measured based upon the value of the asset in relation to the threats and vulnerabilities associated with it. Risk is based on the likelihood or probability of the hazard occurring and the consequences of the occurrence. A risk assessment analyzes the threat (probability of occurrence), and asset value and vulnerabilities (consequences of the occurrence) to ascertain the level of risk for each asset against each applicable threat/hazard. The risk assessment provides engineers and architects with a relative risk profile that defines which assets are at the greatest risk against specific threats. Chapters 2 and 3 explore mitigation measures to reduce the vulnerability and risk for valuable assets with a high risk.

There are numerous methodologies and technologies for conducting a risk assessment. One approach is to assemble the results of the asset value assessment, threat assessment, and vulnerability assessment, and determine a numeric value of risk for each asset and threat/hazard pair in accordance with the following formula:

$$\text{Risk} = \text{Asset Value} \times \text{Threat Rating} \times \text{Vulnerability Rating}$$

This methodology can be used for new buildings during the design process, as well as for existing structures. The first task is to identify the value of assets and people that need to be protected. Next, a threat assessment is performed to identify and define the threats and hazards that could cause harm to a building and its inhabitants. After threats and assets are identified, a vulnerability assessment is performed to identify weaknesses that might be exploited by a terrorist or aggressor. Using the results of the asset value, threat, and vulnerability assessments, risk can be computed.

After the architect and building engineer know how people and assets are at greatest risk against specific threats, they can then identify mitigation measures to reduce risk. Because it is not possible to completely eliminate risk, and every project has resource limitations, architects and engineers must analyze how mitigation measures would affect risk and decide on the best and most cost-effective measures to implement to achieve the desired level of protection (risk management).

There are numerous checklists and techniques to use for conducting an individual building risk assessment. A simplified approach is presented in Tables 1-18 through 1-21. The tables are used as a pre-assessment screening tool by the assessor who conducts an interview with several key staff members (e.g., building owner, security, site management, key function representatives, etc.). The interview provides a consensus judgment of the relative risk or vulnerability of functions or systems and should also identify system interdependencies. Table 1-19 provides both a quantitative score and color code to objectively and visually determine the functions and systems that have been determined to

be at risk. Engineers, architects, or experienced assessors could perform a short walk-through and conduct the pre-assessment interview of an existing building in less than a day. For a new building, the pre-screening results can be used by the designer to focus the design team on incorporating features and redundancies to reduce vulnerabilities and risk.

In the risk assessment approach presented in Tables 1-18 through 1-21, three factors or elements of risk are considered for each function or system against each threat previously identified. The first factor is the value of the asset or degree of debilitating impact that would be caused by the incapacity or destruction of the asset. A value on a scale of 1 to 10 is assigned (as shown in Table 1-18), 1 being a very low impact or consequence and 10 being very high or an exceptionally grave consequence. The next factor is the threat rating or subjective judgment of a terrorist threat based on existence, capability, history, intentions, and targeting. Again, on a scale of 1 to 10, 1 is a very low probability and 10 is a very high probability of a terrorist attack. The third factor of risk is vulnerability, or any weaknesses that can be exploited by an aggressor. A value of 1 to 10 is assigned, 1 being very low or no weaknesses exist, and 10 being very high vulnerability, meaning one or more major weaknesses make an asset extremely susceptible to an aggressor. Multiplying the values assigned to each of the three factors provides quantification of total risk. The total risk for each function or system against each threat is assigned a color code in accordance with Table 1-19. The results of the risk assessment should be used to help prioritize which mitigation measures should be adopted, given limited resources, in order to achieve a desired level of protection.

Table 1-18: Risk Factors Definitions

Very High	10
High	8-9
Medium High	7
Medium	5-6
Medium Low	4
Low	2-3
Very Low	1

Table 1-19: Total Risk Color Code

	Low Risk	Medium Risk	High Risk
Risk Factors Total	1-60	61-175	≥ 176

Table 1-20: Site Functional Pre-Assessment Screening Matrix\*

Function	Cyber Attack	Armed Attack (single gunman)	Vehicle Bomb	CBR Attack
<b>Administration</b>	280	140	135	90
Asset Value	5	5	5	5
Threat Rating	8	4	3	2
Vulnerability Rating	7	7	9	9
<b>Engineering</b>	128	128	192	144
Asset Value	8	8	8	8
Threat Rating	8	4	3	2
Vulnerability Rating	2	4	8	9
<b>Warehousing</b>	96	36	81	54
Asset Value	3	3	3	3
Threat Rating	8	4	3	2
Vulnerability Rating	4	3	9	9
<b>Data Center</b>	360	128	216	144
Asset Value	8	8	8	8
Threat Rating	9	4	3	2
Vulnerability Rating	5	4	9	9



Table 1-20: Site Functional Pre-Assessment Screening Matrix\* (continued)

Function	Cyber Attack	Armed Attack (single gunman)	Vehicle Bomb	CBR Attack
<b>Food Service</b>	2	32	48	36
Asset Value	2	2	2	2
Threat Rating	1	4	3	2
Vulnerability Rating	1	4	8	9
<b>Security</b>	280	140	168	126
Asset Value	7	7	7	7
Threat Rating	8	4	3	2
Vulnerability Rating	5	5	8	9
<b>Housekeeping</b>	16	64	48	36
Asset Value	2	2	2	2
Threat Rating	8	4	3	2
Vulnerability Rating	1	8	8	9
<b>Day Care</b>	54	324	243	162
Asset Value	9	9	9	9
Threat Rating	3	4	3	2
Vulnerability Rating	2	9	9	9

\* NOTIONAL DATA INSERTED FOR DEMONSTRATION PURPOSES.

Table 1-21: Site Infrastructure Systems Pre-Assessment Screening Matrix\*

Function	Cyber Attack	Armed Attack (single gunman)	Vehicle Bomb	CBR Attack
<b>Site</b>	48	80	108	72
Asset Value	4	4	4	4
Threat Rating	4	4	3	2
Vulnerability Rating	3	5	9	9
<b>Architectural</b>	40	40	135	20
Asset Value	5	5	5	5
Threat Rating	8	4	3	2
Vulnerability Rating	1	2	9	2
<b>Structural Systems</b>	24	32	240	16
Asset Value	8	8	8	8
Threat Rating	3	4	3	2
Vulnerability Rating	1	1	10	1
<b>Envelope Systems</b>	84	112	189	112
Asset Value	7	7	7	7
Threat Rating	6	4	3	2
Vulnerability Rating	2	4	9	8

Table 1-21: Site Infrastructure Systems Pre-Assessment Screening Matrix\* (continued)

Function	Cyber Attack	Armed Attack (single gunman)	Vehicle Bomb	CBR Attack
<b>Utility Systems</b>	112	56	168	42
Asset Value	7	7	7	7
Threat Rating	8	4	3	2
Vulnerability Rating	2	2	8	3
<b>Mechanical Systems</b>	42	56	105	126
Asset Value	7	7	7	7
Threat Rating	6	4	3	2
Vulnerability Rating	1	2	5	9
<b>Plumbing and Gas Systems</b>	40	40	120	70
Asset Value	5	5	5	5
Threat Rating	8	4	3	2
Vulnerability Rating	1	2	8	7
<b>Electrical Systems</b>	42	84	189	28
Asset Value	7	7	7	7
Threat Rating	8	4	3	2
Vulnerability Rating	1	3	9	2
<b>Fire Alarm Systems</b>	162	108	216	36
Asset Value	9	9	9	9
Threat Rating	6	4	3	2
Vulnerability Rating	3	3	8	2
<b>IT/Communications Systems</b>	512	64	192	32
Asset Value	8	8	8	8
Threat Rating	8	4	3	2
Vulnerability Rating	8	2	8	2

\* NOTIONAL DATA INSERTED FOR DEMONSTRATION PURPOSES.

The functions and infrastructure analysis will identify the geographic distribution within the building and interdependencies between critical assets. Ideally, the functions should have geographic dispersion as well as a pre-determined recovery site or alternate work location. Similarly, critical infrastructure should have geographic dispersion and backup. Figure 1-10 shows an example of a building that has numerous critical functions and infrastructure collocated, which creates a single-point vulnerability as illustrated below. A bomb or CBR attack entering through the loading dock could impact the telecommunications, data, uninterrupted power supply (UPS), generator, and other key infrastructure systems.

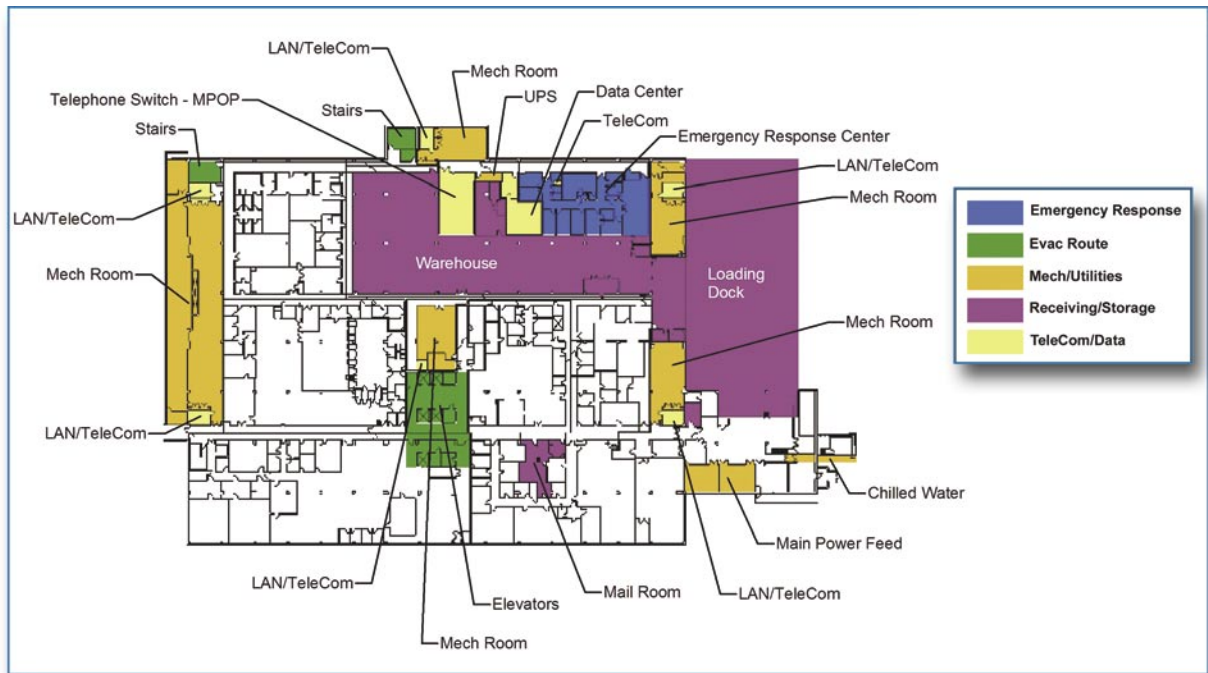


Figure 1-10 Non-redundant critical functions collocated near loading dock

As a minimum, those critical assets assessed to be at highest risk should receive an on-site vulnerability assessment using the Building Vulnerability Assessment Checklist in Table 1-22. The vulnerability assessment may change the risk rating of assets due to the identification of accessible critical nodes, the ease of attack using a common tactic, or some other factor that makes the building more attractive as a target or more susceptible to damage that could result in casualties or irrecoverable system damage. The photographs in Figure 1-11 illustrate some examples of single-point vulnerabilities of systems and infrastructure.



Figure 1-11 Vulnerability examples

## 1.5 RISK MANAGEMENT

Traditionally, the building regulatory system has addressed natural disaster mitigation (hurricane, tornado, flood, earthquake, windstorm, and snow storm) through prescriptive building codes supported by well-established and accepted reference standards, regulations, inspection, and assessment techniques. Some man-made risks (e.g., HazMat storage) and specific societal goals (energy conservation and life safety) have also been similarly addressed. However, the building regulation system has not yet fully addressed most manmade hazards or terrorist threats.

Soon after September 11, 2001, the New York City Building Department initiated an effort to analyze the building code with regard to terrorist threats. The task force issued a report recommending code changes based on the attack on the World Trade Center. The National Fire Protection Association (NFPA) has a committee on premises security and security system installation standards. These advances may some day result in the building regulatory system developing more prescriptive building codes to mitigate security threats.

In the absence of such regulations, the designer needs to understand on what threat the design is based. Just like seismic design requires an understanding of geology, soil structure, and the maximum credible earthquake accelerations possible at a given location, the site designer needs to comprehend the bomb size, vehicle size, and gun or other weapon size to provide an appropriate level of protection. The size of threat and desired level of protection are equally important to the design. For most cases across the United States, the threats and risks for a specific building will be low. For buildings at a higher threat and risk, higher standards and performance may be required. The Department of Defense (DoD), GSA, and DOS all have established processes to identify design basis threats for their facilities.

The typical building design and construction process is sequential, progressing from identifying building use and design goals through actual construction. This process is illustrated in Figure 1-12.



Figure 1-12 Typical building design and construction process

In every design and renovation project, the owner ultimately has three choices when addressing the risk posed by terrorism. He or she can:

1. Do nothing and accept the risk
2. Perform a risk assessment and manage the risk by installing reasonable mitigation measures
3. Harden the building against all threats to achieve the least amount of risk

Figure 1-13 is a graphical representation of the three choices. Since September 11, 2001, terrorism has become a dominant concern. Life, safety, and security issues should be a design goal from the beginning.

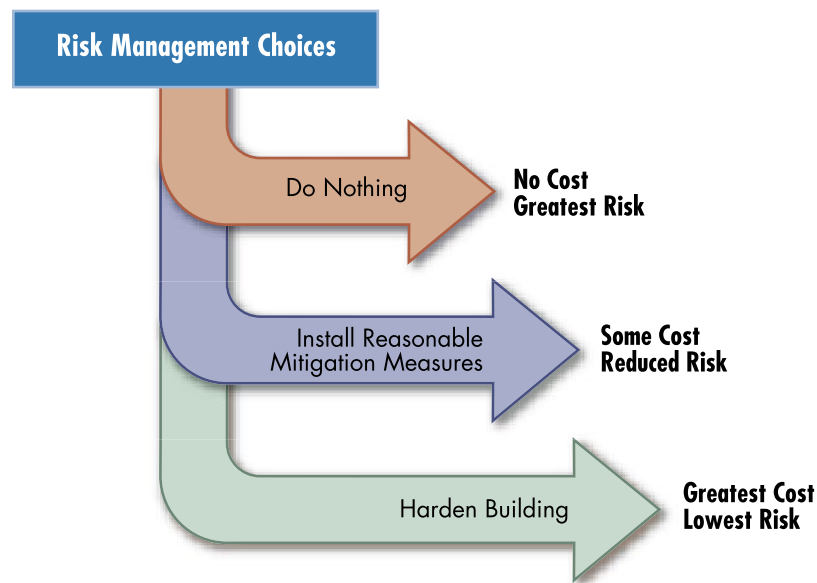


Figure 1-13 Risk management choices

Table 1-22 contains key questions that designers may use to determine vulnerabilities of an existing building or a new construction in order to focus resources and minimize the impacts of potential terrorist attacks or technological accidents.

## **1.6 BUILDING VULNERABILITY ASSESSMENT CHECKLIST**

The Building Vulnerability Assessment Checklist (Table 1-22) is based on the checklist developed by the Department of Veterans Affairs (VA) and compiles many best practices based on technologies and scientific research to consider during the design of a new building or renovation of an existing building. It allows a consistent security evaluation of designs at various levels. The checklist can be used as a screening tool for preliminary design vulnerability assessment. In addition to examining design issues that affect vulnerability, the checklist includes questions that determine if critical systems continue to function in order to enhance deterrence, detection, denial, and damage limitation, and to ensure that emergency systems function during a threat or hazard situation.

The checklist is organized into the 13 sections listed below. To conduct a vulnerability assessment of a building or preliminary design, each section of the checklist should be assigned to an engineer, architect, or subject matter expert who is knowledgeable and qualified to perform an assessment of the assigned area. Each assessor should consider the questions and guidance provided to help identify vulnerabilities and document results in the observations column. If assessing an existing building, vulnerabilities can also be documented with photographs, if possible. The results of the 13 assessments should be integrated into a master vulnerability assessment and provide a basis for determining vulnerability ratings during the assessment process.

1. Site
2. Architectural
3. Structural Systems
4. Building Envelope
5. Utility Systems
6. Mechanical Systems (heating, ventilation, and air conditioning (HVAC) and CBR)
7. Plumbing and Gas Systems
8. Electrical Systems
9. Fire Alarm Systems
10. Communications and Information Technology (IT) Systems
11. Equipment Operations and Maintenance
12. Security Systems
13. Security Master Plan

Table 1-22: Building Vulnerability Assessment Checklist\*

Section	Vulnerability Question	Guidance	Observations
<b>1</b>	<b>Site</b>		
<b>1.1</b>	<p><b>What major structures surround the facility (site or building(s))?</b></p> <p><b>What critical infrastructure, government, military, or recreation facilities are in the local area that impact transportation, utilities, and collateral damage (attack at this facility impacting the other major structures or attack on the major structures impacting this facility)?</b></p> <p><b>What are the adjacent land uses immediately outside the perimeter of this facility (site or building(s))?</b></p>	<p><b>Critical infrastructure to consider includes:</b></p> <p><b>Telecommunications infrastructure</b></p> <p>Facilities for broadcast TV, cable TV; cellular networks; newspaper offices, production, and distribution; radio stations; satellite base stations; telephone trunking and switching stations, including critical cable routes and major rights-of-way</p> <p><b>Electric power systems</b></p> <p>Power plants, especially nuclear facilities; transmission and distribution system components; fuel distribution, delivery, and storage</p> <p><b>Gas and oil facilities</b></p> <p>Hazardous material facilities, oil/gas pipelines, and storage facilities</p>	



Table 1-22: Building Vulnerability Assessment Checklist\* (continued)

Section	Vulnerability Question	Guidance	Observations
	<p><b>Do future development plans change these land uses outside the facility (site or building (s)) perimeter?</b></p> <p>Although this question bridges threat and vulnerability, the threat is the manmade hazard that can occur (likelihood and impact) and the vulnerability is the proximity of the hazard to the building(s) being assessed. Thus, a chemical plant release may be a threat/hazard, but vulnerability changes if the plant is 1 mile upwind for the prevailing winds versus 10 miles away and downwind. Similarly, a terrorist attack upon an adjacent building may impact the building(s) being assessed. The Murrah Federal Building in Oklahoma City was not the only building to have severe damage caused by the explosion of the Ryder rental truck bomb.</p>	<p><b>Banking and finance institutions</b></p> <p>Financial institutions (banks, credit unions) and the business district; note schedule business/financial district may follow; armored car services</p> <p><b>Transportation networks</b></p> <p>Airports: carriers, flight paths, and airport layout; location of air traffic control towers, runways, passenger terminals, and parking areas</p> <p>Bus Stations</p> <p>Pipelines: oil; gas</p> <p>Trains/Subways: rails and lines, railheads/rail yards, interchanges, tunnels, and cargo/passenger terminals; note hazardous material transported</p> <p>Traffic: interstate highways/roads/tunnels/bridges carrying large volumes; points of congestion; note time of day and day of week</p> <p>Trucking: hazardous materials cargo loading/unloading facilities; truck terminals, weigh stations, and rest areas</p> <p>Waterways: dams; levees; berths and ports for cruise ships, ferries, roll-on/roll-off cargo vessels, and container ships; international (foreign) flagged vessels (and cargo)</p> <p><b>Water supply systems</b></p> <p>Pipelines and process/treatment facilities, dams for water collection; wastewater treatment</p> <p><b>Government services</b></p> <p>Federal/state/local government offices — post offices, law enforcement stations, fire/rescue, town/city hall, local mayor's/governor's residences, judicial offices and courts, military installations (include type-Active, Reserves, National Guard)</p> <p><b>Emergency services</b></p> <p>Backup facilities, communications centers, Emergency Operations Centers (EOCs), fire/Emergency Medical Service (EMS) facilities, Emergency Medical Center (EMCs), law enforcement facilities</p>	

Table 1-22: Building Vulnerability Assessment Checklist\* (continued)

Section	Vulnerability Question	Guidance	Observations
		<p><b>The following are not critical infrastructure, but have potential collateral damage to consider:</b></p> <p><b>Agricultural facilities:</b> chemical distribution, storage, and application sites; crop spraying services; farms and ranches; food processing, storage, and distribution facilities</p> <p><b>Commercial/manufacturing/industrial facilities:</b> apartment buildings; business/corporate centers; chemical plants (especially those with Section 302 Extremely Hazardous Substances); factories; fuel production, distribution, and storage facilities; hotels and convention centers; industrial plants; raw material production, distribution, and storage facilities; research facilities and laboratories; shipping, warehousing, transfer, and logistical centers</p> <p><b>Events and attractions:</b> festivals and celebrations; open-air markets; parades; rallies, demonstrations, and marches; religious services; scenic tours; theme parks</p> <p><b>Health care system components:</b> family planning clinics; health department offices; hospitals; radiological material and medical waste transportation, storage, and disposal; research facilities and laboratories, walk-in clinics</p> <p><b>Political or symbolically significant sites:</b> embassies, consulates, landmarks, monuments, political party and special interest groups offices, religious sites</p> <p><b>Public/private institutions:</b> academic institutions, cultural centers, libraries, museums, research facilities and laboratories, schools</p> <p><b>Recreation facilities:</b> auditoriums, casinos, concert halls and pavilions, parks, restaurants and clubs (frequented by potential target populations), sports arenas, stadiums, theaters, malls, and special interest group facilities; note congestion dates and times for shopping centers</p> <p>References: <i>FEMA 386-7, FEMA SLG 101, DOJ NCJ181200</i></p>	
1.2	Does the terrain place the building in a depression or low area?	<p>Depressions or low areas can trap heavy vapors, inhibit natural decontamination by prevailing winds, and reduce the effectiveness of in-place sheltering.</p> <p>Reference: <i>USAF Installation Force Protection Guide</i></p>	

Table 1-22: Building Vulnerability Assessment Checklist\* (continued)

Section	Vulnerability Question	Guidance	Observations
1.3	<b>In dense, urban areas, does curb lane parking allow uncontrolled vehicles to park unacceptably close to a building in public rights-of-way?</b>	<p>Where distance from the building to the nearest curb provides insufficient setback, restrict parking in the curb lane. For typical city streets, this may require negotiating to close the curb lane. Setback is common terminology for the distance between a building and its associated roadway or parking. It is analogous to stand-off between a vehicle bomb and the building. The benefit per foot of increased stand-off between a potential vehicle bomb and a building is very high when close to a building and decreases rapidly as the distance increases. Note that the July 1, 1994, Americans with Disabilities Act Standards for Accessible Design states that required handicapped parking shall be located on the shortest accessible route of travel from adjacent parking to an accessible entrance.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
1.4	<b>Is a perimeter fence or other types of barrier controls in place?</b>	<p>The intent is to channel pedestrian traffic onto a site with multiple buildings through known access control points. For a single building, the intent is to have a single visitor entrance.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
1.5	<b>What are the site access points to the site or building?</b>	<p>The goal is to have at least two access points — one for passenger vehicles and one for delivery trucks due to the different procedures needed for each. Having two access points also helps if one of the access points becomes unusable, then traffic can be routed through the other access point.</p> <p>Reference: <i>USAF Installation Force Protection Guide</i></p>	
1.6	<b>Is vehicle traffic separated from pedestrian traffic on the site?</b>	<p>Pedestrian access should not be endangered by car traffic. Pedestrian access, especially from public transportation, should not cross vehicle traffic if possible.</p> <p>References: <i>GSA PBS-P100 and FEMA 386-7</i></p>	
1.7	<b>Is there vehicle and pedestrian access control at the perimeter of the site?</b>	<p>Vehicle and pedestrian access control and inspection should occur as far from facilities as possible (preferably at the site perimeter) with the ability to regulate the flow of people and vehicles one at a time.</p> <p>Control on-site parking with identification checks, security personnel, and access control systems.</p> <p>Reference: <i>FEMA 386-7</i></p>	

Table 1-22: Building Vulnerability Assessment Checklist\* (continued)

Section	Vulnerability Question	Guidance	Observations
1.8	<p><b>Is there space for inspection at the curb line or outside the protected perimeter?</b></p> <p><b>What is the minimum distance from the inspection location to the building?</b></p>	<p>Design features for the vehicular inspection point include: vehicle arrest devices that prevent vehicles from leaving the vehicular inspection area and prevent tailgating.</p> <p>If screening space cannot be provided, consider other design features such as: hardening and alternative location for vehicle search/inspection.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
1.9	<p><b>Is there any potential access to the site or building through utility paths or water runoff?</b></p>	<p>Eliminate potential site access through utility tunnels, corridors, manholes, stormwater runoff culverts, etc. Ensure covers to these access points are secured.</p> <p>Reference: <i>USAF Installation Force Protection Guide</i></p>	
1.10	<p><b>What are the existing types of vehicle anti-ram devices for the site or building?</b></p> <p><b>Are these devices at the property boundary or at the building?</b></p>	<p>Passive barriers include bollards, walls, hardened fences (steel cable interlaced), trenches, ponds/basins, concrete planters, street furniture, plantings, trees, sculptures, and fountains. Active barriers include pop-up bollards, swing arm gates, and rotating plates and drums, etc.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
1.11	<p><b>What is the anti-ram buffer zone stand-off distance from the building to unscreened vehicles or parking?</b></p>	<p>If the recommended distance for the postulated threat is not available, consider reducing the stand-off required through structural hardening or manufacturing additional stand-off through barriers and parking restrictions. Also, consider relocation of vulnerable functions within the building, or to a more hazard-resistant building. More stand-off should be used for unscreened vehicles than for screened vehicles that have been searched.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
1.12	<p><b>Are perimeter barriers capable of stopping vehicles?</b></p> <p><b>Will the vehicle barriers at the perimeter and building maintain access for emergency responders, including large fire apparatus?</b></p>	<p>Anti-ram protection may be provided by adequately designed: bollards, street furniture, sculpture, landscaping, walls, and fences. The anti-ram protection must be able to stop the threat vehicle size (weight) at the speed attainable by that vehicle at impact. If the anti-ram protection cannot absorb the desired kinetic energy, consider adding speed controls (serpentines or speed bumps) to limit the speed at impact. If the resultant speed is still too great, the anti-ram protection should be improved.</p> <p>References: <i>Military Handbook 1013/14 and GSA PBS P-100</i></p>	

Table 1-22: Building Vulnerability Assessment Checklist\* (continued)

Section	Vulnerability Question	Guidance	Observations
1.13	<b>Does site circulation prevent high-speed approaches by vehicles?</b>	The intent is to use site circulation to minimize vehicle speeds and eliminate direct approaches to structures.  Reference: <i>GSA PBS-P100</i>	
1.14	<b>Are there offsetting vehicle entrances from the direction of a vehicle's approach to force a reduction of speed?</b>	Single or double 90-degree turns effectively reduce vehicle approach speed.  Reference: <i>GSA PBS-P100</i>	
1.15	<b>Is there a minimum setback distance between the building and parked vehicles?</b>	Adjacent public parking should be directed to more distant or better-protected areas, segregated from employee parking and away from the building. Some publications use the term setback in lieu of the term stand-off.  Reference: <i>GSA PBS-P100</i>	
1.16	<b>Does adjacent surface parking on site maintain a minimum stand-off distance?</b>	The specific stand-off distance needed is based upon the design basis threat bomb size and the building construction. For initial screening, consider using 25 meters (82 feet) as a minimum, with more distance needed for unreinforced masonry or wooden walls.  Reference: <i>GSA PBS-P100</i>	
1.17	<b>Do standalone, aboveground parking garages provide adequate visibility across as well as into and out of the parking garage?</b>	Pedestrian paths should be planned to concentrate activity to the extent possible.  Limiting vehicular entry/exits to a minimum number of locations is beneficial.  Stair tower and elevator lobby design should be as open as code permits. Stair and/or elevator waiting areas should be as open to the exterior and/or the parking areas as possible and well lighted. Impact-resistant, laminated glass for stair towers and elevators is a way to provide visual openness.  Potential hiding places below stairs should be closed off; nooks and crannies should be avoided, and dead-end parking areas should be eliminated.  Reference: <i>GSA PBS-P100</i>	
1.18	<b>Are garage or service area entrances for employee-permitted vehicles protected by suitable anti-ram devices?</b>  <b>Coordinate this protection with other anti-ram devices, such as on the perimeter or property boundary to avoid duplication of arresting capability.</b>	Control internal building parking, underground parking garages, and access to service areas and loading docks in this manner with proper access control, or eliminate the parking altogether.  The anti-ram device must be capable of arresting a vehicle of the designated threat size at the speed attainable at the location.  Reference: <i>GSA PBS-P100</i>	

Table 1-22: Building Vulnerability Assessment Checklist\* (continued)

Section	Vulnerability Question	Guidance	Observations
1.19	<b>Do site landscaping and street furniture provide hiding places?</b>	<p>Minimize concealment opportunities by keeping landscape plantings (hedges, shrubbery, and large plants with heavy ground cover) and street furniture (bus shelters, benches, trash receptacles, mailboxes, newspaper vending machines) away from the building to permit observation of intruders and prevent hiding of packages.</p> <p>If mail or express boxes are used, the size of the openings should be restricted to prohibit the insertion of packages.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
1.20	<b>Is the site lighting adequate from a security perspective in roadway access and parking areas?</b>	<p>Security protection can be successfully addressed through adequate lighting. The type and design of lighting, including illumination levels, is critical. Illuminating Engineering Society of North America (IESNA) guidelines can be used. The site lighting should be coordinated with the CCTV system.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
1.21	<b>Are line-of-sight perspectives from outside the secured boundary to the building and on the property along pedestrian and vehicle routes integrated with landscaping and green space?</b>	<p>The goal is to prevent the observation of critical assets by persons outside the secure boundary of the site. For individual buildings in an urban environment, this could mean appropriate window treatments or no windows for portions of the building.</p> <p>Once on the site, the concern is to ensure observation by a general workforce aware of any pedestrians or vehicles outside normal circulation routes or attempting to approach the building unobserved.</p> <p>Reference: <i>USAF Installation Force Protection Guide</i></p>	
1.22	<b>Do signs provide control of vehicles and people?</b>	<p>The signage should be simple and have the necessary level of clarity. However, signs that identify sensitive areas should generally not be provided.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
1.23	<b>Are all existing fire hydrants on the site accessible?</b>	<p>Just as vehicle access points to the site must be able to transit emergency vehicles, so too must the emergency vehicles have access to the buildings and, in the case of fire trucks, the fire hydrants. Thus, security considerations must accommodate emergency response requirements.</p> <p>Reference: <i>GSA PBS-P100</i></p>	

Table 1-22: Building Vulnerability Assessment Checklist\* (continued)

Section	Vulnerability Question	Guidance	Observations
<b>2</b>	<b>Architectural</b>		
<b>2.1</b>	<b>Does the site and architectural design incorporate strategies from a Crime Prevention Through Environmental Design (CPTED) perspective?</b>	<p><b>The focus of CPTED is on creating defensible space by employing:</b></p> <ol style="list-style-type: none"> <li><b>1. Natural access controls:</b> <ul style="list-style-type: none"> <li>Design streets, sidewalks, and building entrances to clearly indicate public routes and direct people away from private/restricted areas</li> <li>Discourage access to private areas with structural elements and limit access (no cut-through streets)</li> <li>Loading zones should be separate from public parking</li> </ul> </li> <li><b>2. Natural surveillance:</b> <ul style="list-style-type: none"> <li>Design that maximizes visibility of people, parking areas, and building entrances; doors and windows that look out on to streets and parking areas</li> <li>Shrubby under 2 feet in height for visibility</li> <li>Lower branches of existing trees kept at least 10 feet off the ground</li> <li>Pedestrian-friendly sidewalks and streets to control pedestrian and vehicle circulation</li> <li>Adequate nighttime lighting, especially at exterior doorways</li> </ul> </li> <li><b>3. Territorial reinforcement:</b> <ul style="list-style-type: none"> <li>Design that defines property lines</li> <li>Design that distinguishes private/restricted spaces from public spaces using separation, landscape plantings; pavement designs (pathway and roadway placement); gateway treatments at lobbies, corridors, and door placement; walls, barriers, signage, lighting, and "CPTED" fences</li> <li>"Traffic-calming" devices for vehicle speed control</li> </ul> </li> <li><b>4. Target hardening:</b> <ul style="list-style-type: none"> <li>Prohibit entry or access: window locks, deadbolts for doors, interior door hinges</li> <li>Access control (building and employee/visitor parking) and intrusion detection systems</li> </ul> </li> <li><b>5. Closed circuit television cameras:</b> <ul style="list-style-type: none"> <li>Prevent crime and influence positive behavior, while enhancing the intended uses of space. In other words, design that eliminates or reduces criminal behavior and at the same time encourages people to "keep an eye out" for each other.</li> </ul> </li> </ol> <p>References: GSA PBS-P100 and FEMA 386-7</p>	

Table 1-22: Building Vulnerability Assessment Checklist\* (continued)

Section	Vulnerability Question	Guidance	Observations
2.2	<b>Is it a mixed-tenant building?</b>	<p>Separate high-risk tenants from low-risk tenants and from publicly accessible areas. Mixed uses may be accommodated through such means as separating entryways, controlling access, and hardening shared partitions, as well as through special security operational countermeasures.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
2.3	<b>Are pedestrian paths planned to concentrate activity to aid in detection?</b>	<p>Site planning and landscape design can provide natural surveillance by concentrating pedestrian activity, limiting entrances/exits, and eliminating concealment opportunities. Also, prevent pedestrian access to parking areas other than via established entrances.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
2.4	<b>Are there trash receptacles and mailboxes in close proximity to the building that can be used to hide explosive devices?</b>	<p>The size of the trash receptacles and mailbox openings should be restricted to prohibit insertion of packages. Street furniture, such as newspaper vending machines, should be kept sufficient distance (10 meters or 33 feet) from the building, or brought inside to a secure area.</p> <p>References: <i>USAF Installation Force Protection Guide and DoD UCF 4-010-01</i></p>	
2.5	<b>Do entrances avoid significant queuing?</b>	<p>If queuing will occur within the building footprint, the area should be enclosed in blast-resistant construction. If queuing is expected outside the building, a rain cover should be provided. For manpower and equipment requirements, collocate or combine staff and visitor entrances.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
2.6	<p><b>Does security screening cover all public and private areas?</b></p> <p><b>Are public and private activities separated?</b></p> <p><b>Are public toilets, service spaces, or access to stairs or elevators located in any non-secure areas, including the queuing area before screening at the public entrance?</b></p>	<p>Retail activities should be prohibited in non-secured areas. However, the Public Building Cooperative Use Act of 1976 encourages retail and mixed uses to create open and inviting buildings. Consider separating entryways, controlling access, hardening shared partitions, and special security operational countermeasures.</p> <p>References: <i>GSA PBS-P100 and FEMA 386-7</i></p>	



Table 1-22: Building Vulnerability Assessment Checklist\* (continued)

Section	Vulnerability Question	Guidance	Observations
2.7	<p><b>Is access control provided through main entrance points for employees and visitors?</b></p> <p>(lobby receptionist, sign-in, staff escorts, issue of visitor badges, checking forms of personal identification, electronic access control systems)</p>	<p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
2.8	<p><b>Is access to private and public space or restricted area space clearly defined through the design of the space, signage, use of electronic security devices, etc.?</b></p>	<p>Finishes and signage should be designed for visual simplicity.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
2.9	<p><b>Is access to elevators distinguished as to those that are designated only for employees and visitors?</b></p>	<p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
2.10	<p><b>Do public and employee entrances include space for possible future installation of access control and screening equipment?</b></p>	<p>These include walk-through metal detectors and x-ray devices, identification check, electronic access card, search stations, and turnstiles.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
2.11	<p><b>Do foyers have reinforced concrete walls and offset interior and exterior doors from each other?</b></p>	<p>Consider for exterior entrances to the building or to access critical areas within the building if explosive blast hazard must be mitigated.</p> <p>Reference: <i>U.S. Army TM 5-853</i></p>	
2.12	<p><b>Do doors and walls along the line of security screening meet requirements of UL752 "Standard for Safety: Bullet-Resisting Equipment"?</b></p>	<p>If the postulated threat in designing entrance access control includes rifles, pistols, or shotguns, then the screening area should have bullet-resistance to protect security personnel and uninvolved bystanders. Glass, if present, should also be bullet-resistant.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
2.13	<p><b>Do circulation routes have unobstructed views of people approaching controlled access points?</b></p>	<p>This applies to building entrances and to critical areas within the building.</p> <p>References: <i>USAF Installation Force Protection Guide and DoD UFC 4-010-01</i></p>	

Table 1-22: Building Vulnerability Assessment Checklist\* (continued)

Section	Vulnerability Question	Guidance	Observations
2.14	Is roof access limited to authorized personnel by means of locking mechanisms?	References: <i>GSA PBS-P100</i> and <i>CDC/NIOSH, Pub 2002-139</i>	
2.15	<p>Are critical assets (people, activities, building systems and components) located close to any main entrance, vehicle circulation, parking, maintenance area, loading dock, or interior parking?</p> <p>Are the critical building systems and components hardened?</p>	<p>Critical building components include: Emergency generator including fuel systems, day tank, fire sprinkler, and water supply; Normal fuel storage; Main switchgear; Telephone distribution and main switchgear; Fire pumps; Building control centers; Uninterruptible Power Supply (UPS) systems controlling critical functions; Main refrigeration and ventilation systems if critical to building operation; Elevator machinery and controls; Shafts for stairs, elevators, and utilities; Critical distribution feeders for emergency power. Evacuation and rescue require emergency systems to remain operational during a disaster and they should be located away from potential attack locations. Primary and backup systems should be separated to reduce the risk of both being impacted by a single incident if collocated. Utility systems should be located at least 50 feet from loading docks, front entrances, and parking areas.</p> <p>One way to harden critical building systems and components is to enclose them within hardened walls, floors, and ceilings. Do not place them near high-risk areas where they can receive collateral damage.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
2.16	Are high-value or critical assets located as far into the interior of the building as possible and separated from the public areas of the building?	<p>Critical assets, such as people and activities, are more vulnerable to hazards when on an exterior building wall or adjacent to uncontrolled public areas inside the building.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
2.17	Is high visitor activity away from critical assets?	<p>High-risk activities should also be separated from low-risk activities. Also, visitor activities should be separated from daily activities.</p> <p>Reference: <i>USAF Installation Force Protection Guide</i></p>	
2.18	<p>Are critical assets located in spaces that are occupied 24 hours per day?</p> <p>Are assets located in areas where they are visible to more than one person?</p>	Reference: <i>USAF Installation Force Protection Guide</i>	

Table 1-22: Building Vulnerability Assessment Checklist\* (continued)

Section	Vulnerability Question	Guidance	Observations
2.19	<b>Are loading docks and receiving and shipping areas separated in any direction from utility rooms, utility mains, and service entrances, including electrical, telephone/data, fire detection/ alarm systems, fire suppression water mains, cooling and heating mains, etc.?</b>	<p>Loading docks should be designed to keep vehicles from driving into or parking under the building. If loading docks are in close proximity to critical equipment, consider hardening the equipment and service against explosive blast. Consider a 50-foot separation distance in all directions.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
2.20	<b>Are mailrooms located away from building main entrances, areas containing critical services, utilities, distribution systems, and important assets?</b>  <b>Is the mailroom located near the loading dock?</b>	<p>The mailroom should be located at the perimeter of the building with an outside wall or window designed for pressure relief.</p> <p>By separating the mailroom and the loading dock, the collateral damage of an incident at one has less impact upon the other. However, this may be the preferred mailroom location.</p> <p>Off-site screening stations or a separate delivery processing building on site may be cost-effective, particularly if several buildings may share one mailroom. A separate delivery processing building reduces risk and simplifies protection measures.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
2.21	<b>Does the mailroom have adequate space available for equipment to examine incoming packages and for an explosive disposal container?</b>	<p>Screening of all deliveries to the building, including U.S. mail, commercial package delivery services, delivery of office supplies, etc.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
2.22	<b>Are areas of refuge identified, with special consideration given to egress?</b>	<p>Areas of refuge can be safe havens, shelters, or protected spaces for use during specified hazards.</p> <p>Reference: <i>FEMA 386-7</i></p>	
2.23	<b>Are stairwells required for emergency egress located as remotely as possible from high-risk areas where blast events might occur?</b>  <b>Are stairways maintained with positive pressure or are there other smoke control systems?</b>	<p>Consider designing stairs so that they discharge into areas other than lobbies, parking, or loading docks.</p> <p>Maintaining positive pressure from a clean source of air (may require special filtering) aids in egress by keeping smoke, heat, toxic fumes, etc., out of the stairway. Pressurize exit stairways in accordance with the National Model Building Code.</p> <p>References: <i>GSA PBS-P100 and CDC/NIOSH, Pub 2002-139</i></p>	

Table 1-22: Building Vulnerability Assessment Checklist\* (continued)

Section	Vulnerability Question	Guidance	Observations
2.24	<b>Are enclosures for emergency egress hardened to limit the extent of debris that might otherwise impede safe passage and reduce the flow of evacuees?</b>	Egress pathways should be hardened and discharge into safe areas.  Reference: <i>FEMA 386-7</i>	
2.25	<b>Do interior barriers differentiate level of security within a building?</b>	Reference: <i>USAF Installation Force Protection Guide</i>	
2.26	<b>Are emergency systems located away from high-risk areas?</b>	The intent is to keep the emergency systems out of harm's way, such that one incident does not take out all capability – both the regular systems and their backups.	
2.27	<b>Is interior glazing near high-risk areas minimized?</b>  <b>Is interior glazing in other areas shatter-resistant?</b>	Reference: <i>FEMA 386-7</i>  Interior glazing should be minimized where a threat exists and should be avoided in enclosures of critical functions next to high-risk areas.  Reference: <i>GSA PBS-P100</i>	
2.28	<b>Are ceiling and lighting systems designed to remain in place during hazard events?</b>	When an explosive blast shatters a window, the blast wave enters the interior space, putting structural and non-structural building components under loads not considered in standard building codes. It has been shown that connection criteria for these systems in high seismic activity areas resulted in much less falling debris that could injure building occupants.  Mount all overhead utilities and other fixtures weighing 14 kilograms (31 pounds) or more to minimize the likelihood that they will fall and injure building occupants. Design all equipment mountings to resist forces of 0.5 times the equipment weight in any direction and 1.5 times the equipment weight in the downward direction. This standard does not preclude the need to design equipment mountings for forces required by other criteria, such as seismic standards.  Reference: <i>DoD UCF 4-101-01</i>	

Table 1-22: Building Vulnerability Assessment Checklist\* (continued)

Section	Vulnerability Question	Guidance	Observations
<b>3</b>	<b>Structural Systems</b>		
<b>3.1</b>	<b>What type of construction?</b>  <b>What type of concrete and reinforcing steel?</b>  <b>What type of steel?</b>  <b>What type of foundation?</b>	<p>The type of construction provides an indication of the robustness to abnormal loading and load reversals. A reinforced concrete moment-resisting frame provides greater ductility and redundancy than a flat-slab or flat-plate construction. The ductility of steel frame with metal deck depends on the connection details and pre-tensioned or post-tensioned construction provides little capacity for abnormal loading patterns and load reversals. The resistance of load-bearing wall structures varies to a great extent, depending on whether the walls are reinforced or un-reinforced. A rapid screening process developed by FEMA for assessing structural hazards identifies the following types of construction with a structural score ranging from 1.0 to 8.5. A higher score indicates a greater capacity to sustain load reversals.</p> <p>Wood buildings of all types - 4.5 to 8.5  Steel moment-resisting frames - 3.5 to 4.5  Braced steel frames - 2.5 to 3.0  Light metal buildings - 5.5 to 6.5  Steel frames with cast-in-place concrete shear walls - 3.5 to 4.5  Steel frames with unreinforced masonry infill walls - 1.5 to 3.0  Concrete moment-resisting frames - 2.0 to 4.0  Concrete shear wall buildings - 3.0 to 4.0  Concrete frames with unreinforced masonry infill walls - 1.5 to 3.0  Tilt-up buildings - 2.0 to 3.5  Precast concrete frame buildings - 1.5 to 2.5  Reinforced masonry - 3.0 to 4.0  Unreinforced masonry - 1.0 to 2.5</p> <p>References: <i>FEMA 154 and Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
<b>3.2</b>	<b>Do the reinforced concrete structures contain symmetric steel reinforcement (positive and negative faces) in all floor slabs, roof slabs, walls, beams, and girders that may be subjected to rebound, uplift, and suction pressures?</b>	Reference: <i>GSA PBS-P100</i>	

Table 1-22: Building Vulnerability Assessment Checklist\* (continued)

Section	Vulnerability Question	Guidance	Observations
	<p><b>Do the lap splices fully develop the capacity of the reinforcement?</b></p> <p><b>Are lap splices and other discontinuities staggered?</b></p> <p><b>Do the connections possess ductile details?</b></p> <p><b>Is special shear reinforcement, including ties and stirrups, available to allow large post-elastic behavior?</b></p>		
3.3	<p><b>Are the steel frame connections moment connections?</b></p> <p><b>Is the column spacing minimized so that reasonably sized members will resist the design loads and increase the redundancy of the system?</b></p> <p><b>What are the floor-to-floor heights?</b></p>	<p>A practical upper level for column spacing is generally 30 feet. Unless there is an overriding architectural requirement, a practical limit for floor-to-floor heights is generally less than or equal to 16 feet.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
3.4	<p><b>Are critical elements vulnerable to failure?</b></p>	<p>The priority for upgrades should be based on the relative importance of structural or non-structural elements that are essential to mitigating the extent of collapse and minimizing injury and damage.</p> <p>Primary Structural Elements provide the essential parts of the building's resistance to catastrophic blast loads and progressive collapse. These include columns, girders, roof beams, and the main lateral resistance system.</p> <p>Secondary Structural Elements consist of all other load-bearing members, such as floor beams, slabs, etc.</p> <p>Primary Non-Structural Elements consist of elements (including their attachments) that are essential for life safety systems or elements that can cause substantial injury if failure occurs, including ceilings or heavy suspended mechanical units.</p> <p>Secondary Non-Structural Elements consist of all elements not covered in primary non-structural elements, such as partitions, furniture, and light fixtures.</p> <p>Reference: <i>GSA PBS-P100</i></p>	

Table 1-22: Building Vulnerability Assessment Checklist\* (continued)

Section	Vulnerability Question	Guidance	Observations
3.5	Will the structure suffer an unacceptable level of damage resulting from the postulated threat (blast loading or weapon impact)?	<p>The extent of damage to the structure and exterior wall systems from the bomb threat may be related to a protection level. The following is for new buildings:</p> <p><b>Level of Protection Below Antiterrorism Standards</b> – Severe damage. Frame collapse/massive destruction. Little left standing. Doors and windows fail and result in lethal hazards. Majority of personnel suffer fatalities.</p> <p><b>Very Low Level Protection</b> – Heavy damage. Onset of structural collapse. Major deformation of primary and secondary structural members, but progressive collapse is unlikely. Collapse of non-structural elements. Glazing will break and is likely to be propelled into the building, resulting in serious glazing fragment injuries, but fragments will be reduced. Doors may be propelled into rooms, presenting serious hazards. Majority of personnel suffer serious injuries. There are likely to be a limited number (10 percent to 25 percent) of fatalities.</p> <p><b>Low Level of Protection</b> – Moderate damage, unrepairable. Major deformation of non-structural elements and secondary structural members and minor deformation of primary structural members, but progressive collapse is unlikely. Glazing will break, but fall within 1 meter of the wall or otherwise not present a significant fragment hazard. Doors may fail, but they will rebound out of their frames, presenting minimal hazards. Majority of personnel suffer significant injuries. There may be a few (&lt;10 percent) fatalities.</p> <p><b>Medium Level Protection</b> – Minor damage, repairable. Minor deformations of non-structural elements and secondary structural members and no permanent deformation in primary structural members. Glazing will break, but will remain in the window frame. Doors will stay in frames, but will not be reusable. Some minor injuries, but fatalities are unlikely.</p> <p><b>High Level Protection</b> – Minimal damage, repairable. No permanent deformation of primary and secondary structural members or non-structural elements. Glazing will not break. Doors will be reusable. Only superficial injuries are likely.</p> <p>Reference: DoD UFC 4-010-01</p>	
3.6	<p>Is the structure vulnerable to progressive collapse?</p> <p>Is the building capable of sustaining the removal of a column for one floor above grade at</p>	<p>Design to mitigate progressive collapse is an independent analysis to determine a system's ability to resist structural collapse upon the loss of a major structural element or the system's ability to resist the loss of a major structural element. Design to mitigate progressive collapse may be based on the methods outlined in ASCE 7-98 (now 7-02). Designers may apply static and/or</p>	

Table 1-22: Building Vulnerability Assessment Checklist\* (continued)

Section	Vulnerability Question	Guidance	Observations
	<p><b>the building perimeter without progressive collapse?</b></p> <p><b>In the event of an internal explosion in an uncontrolled public ground floor area, does the design prevent progressive collapse due to the loss of one primary column?</b></p> <p><b>Do architectural or structural features provide a minimum 6-inch stand-off to the internal columns (primary vertical load carrying members)?</b></p> <p><b>Are the columns in the unscreened internal spaces designed for an unbraced length equal to two floors, or three floors where there are two levels of parking?</b></p>	<p>dynamic methods of analysis to meet this requirement and ultimate load capacities may be assumed in the analyses. Combine structural upgrades for retrofits to existing buildings, such as seismic and progressive collapse, into a single project due to the economic synergies and other cross benefits. Existing facilities may be retrofitted to withstand the design level threat or to accept the loss of a column for one floor above grade at the building perimeter without progressive collapse. Note that collapse of floors or roof must not be permitted.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
3.7	<b>Are there adequate redundant load paths in the structure?</b>	<p>Special consideration should be given to materials that have inherent ductility and that are better able to respond to load reversals, such as cast in place reinforced concrete, reinforced masonry, and steel construction.</p> <p>Careful detailing is required for material such as pre-stressed concrete, pre-cast concrete, and masonry to adequately respond to the design loads. Primary vertical load carrying members should be protected where parking is inside a facility and the building superstructure is supported by the parking structure.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
3.8	<b>Are there transfer girders supported by columns within unscreened public spaces or at the exterior of the building?</b>	<p>Transfer girders allow discontinuities in columns between the roof and foundation. This design has inherent difficulty in transferring load to redundant paths upon loss of a column or the girder. Transfer beams and girders that, if lost, may cause progressive collapse are highly discouraged.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
3.9	<b>What is the grouting and reinforcement of masonry (brick and/or concrete masonry unit (CMU)) exterior walls?</b>	<p>Avoid unreinforced masonry exterior walls. Reinforcement can run the range of light to heavy, depending upon the stand-off distance available and postulated design threat.</p> <p>Reference: <i>GSA PBS-P100</i> recommends fully grouted and reinforced CMU construction where CMU is selected.</p>	



Table 1-22: Building Vulnerability Assessment Checklist\* (continued)

Section	Vulnerability Question	Guidance	Observations
		Reference: <i>DoD Minimum Antiterrorism Standards for Buildings</i> states "Unreinforced masonry walls are prohibited for the exterior walls of new buildings. A minimum of 0.05 percent vertical reinforcement with a maximum spacing of 1200 mm (48 in) will be provided. For existing buildings, implement mitigating measures to provide an equivalent level of protection." [This is light reinforcement and based upon the recommended stand-off distance for the situation.]	
3.10	Will the loading dock design limit damage to adjacent areas and vent explosive force to the exterior of the building?	Design the floor of the loading dock for blast resistance if the area below is occupied or contains critical utilities.  Reference: <i>GSA PBS-P100</i>	
3.11	Are mailrooms, where packages are received and opened for inspection, and unscreened retail spaces designed to mitigate the effects of a blast on primary vertical or lateral bracing members?	Where mailrooms and unscreened retail spaces are located in occupied areas or adjacent to critical utilities, walls, ceilings, and floors, they should be blast- and fragment- resistant.  Methods to facilitate the venting of explosive forces and gases from the interior spaces to the outside of the structure may include blow-out panels and window system designs that provide protection from blast pressure applied to the outside, but that readily fail and vent if exposed to blast pressure on the inside.  Reference: <i>GSA PBS-P100</i>	
<b>4 Building Envelope</b>			
4.1	What is the designed or estimated protection level of the exterior walls against the postulated explosive threat?	The performance of the façade varies to a great extent on the materials. Different construction includes brick or stone with block backup, steel stud walls, precast panels, or curtain wall with glass, stone, or metal panel elements.  Shear walls that are essential to the lateral and vertical load bearing system and that also function as exterior walls should be considered primary structures and should resist the actual blast loads predicted from the threats specified. Where exterior walls are not designed for the full design loads, special consideration should be given to construction types that reduce the potential for injury.  Reference: <i>GSA PBS-P100</i>	

Table 1-22: Building Vulnerability Assessment Checklist\* (continued)

Section	Vulnerability Question	Guidance	Observations
4.2	<p><b>Is there less than a 40 percent fenestration opening per structural bay?</b></p> <p><b>Is the window system design on the exterior façade balanced to mitigate the hazardous effects of flying glazing following an explosive event? (glazing, frames, anchorage to supporting walls, etc.)</b></p> <p><b>Do the glazing systems with a ½-inch (¾-inch is better) bite contain an application of structural silicone?</b></p> <p><b>Is the glazing laminated or is it protected with an anti-shatter (fragment retention) film?</b></p> <p><b>If an anti-shatter film is used, is it a minimum of a 7-mil thick film, or specially manufactured 4-mil thick film?</b></p>	<p>The performance of the glass will similarly depend on the materials. Glazing may be single pane or double pane, monolithic or laminated, annealed, heat strengthened or fully tempered.</p> <p>The percent fenestration is a balance between protection level, cost, the architectural look of the building within its surroundings, and building codes. One goal is to keep fenestration to below 40 percent of the building envelope vertical surface area, but the process must balance differing requirements. A blast engineer may prefer no windows; an architect may favor window curtain walls; building codes require so much fenestration per square footage of floor area; fire codes require a prescribed window opening area if the window is a designated escape route; and the building owner has cost concerns.</p> <p>Ideally, an owner would want 100 percent of the glazed area to provide the design protection level against the postulated explosive threat (design basis threat— weapon size at the expected stand-off distance). However, economics and geometry may allow 80 percent to 90 percent due to the statistical differences in the manufacturing process for glass or the angle of incidence of the blast wave upon upper story windows (4th floor and higher).</p> <p>Reference: <i>GSA PBS-P100</i></p>	
4.3	<p><b>Do the walls, anchorage, and window framing fully develop the capacity of the glazing material selected?</b></p> <p><b>Are the walls capable of withstanding the dynamic reactions from the windows?</b></p> <p><b>Will the anchorage remain attached to the walls of the building during an explosive event without failure?</b></p> <p><b>Is the façade connected to backup block or to the structural frame?</b></p> <p><b>Are non-bearing masonry walls reinforced?</b></p>	<p>Government produced and sponsored computer programs coupled with test data and recognized dynamic structural analysis techniques may be used to determine whether the glazing either survives the specified threats or the post damage performance of the glazing protects the occupants. A breakage probability no higher than 750 breaks per 1,000 may be used when calculating loads to frames and anchorage.</p> <p>The intent is to ensure the building envelope provides relatively equal protection against the postulated explosive threat for the walls and window systems for the safety of the occupants, especially in rooms with exterior walls.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
4.4	<p><b>Does the building contain ballistic glazing?</b></p>	<p>Glass-clad polycarbonate or laminated polycarbonate are two types of acceptable glazing material.</p>	

Table 1-22: Building Vulnerability Assessment Checklist\* (continued)

Section	Vulnerability Question	Guidance	Observations
	<p><b>Does the ballistic glazing meet the requirements of UL 752 Bullet-Resistant Glazing?</b></p> <p><b>Does the building contain security-glazing?</b></p> <p><b>Does the security-glazing meet the requirements of ASTM F1233 or UL 972, Burglary Resistant Glazing Material?</b></p> <p><b>Do the window assemblies containing forced entry resistant glazing (excluding the glazing) meet the requirements of ASTM F 588?</b></p>	<p>If windows are upgraded to bullet-resistant, burglar-resistant, or forced entry-resistant, ensure that doors, ceilings, and floors, as applicable, can resist the same for the areas of concern.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
4.5	<p><b>Do non-window openings, such as mechanical vents and exposed plenums, provide the same level of protection required for the exterior wall?</b></p>	<p>In-filling of blast over-pressures must be considered through non-window openings such that structural members and all mechanical system mountings and attachments should resist these interior fill pressures.</p> <p>These non-window openings should also be as secure as the rest of the building envelope against forced entry.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
<b>5 Utility Systems</b>			
5.1	<p><b>What is the source of domestic water? (utility, municipal, wells, lake, river, storage tank)</b></p> <p><b>Is there a secure alternate drinking water supply?</b></p>	<p>Domestic water is critical for continued building operation. Although bottled water can satisfy requirements for drinking water and minimal sanitation, domestic water meets many other needs – flushing toilets, building heating and cooling system operation, cooling of emergency generators, humidification, etc.</p> <p>Reference: <i>FEMA 386-7</i></p>	
5.2	<p><b>Are there multiple entry points for the water supply?</b></p>	<p>If the building or site has only one source of water entering at one location, the entry point should be secure.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
5.3	<p><b>Is the incoming water supply in a secure location?</b></p>	<p>Ensure that only authorized personnel have access to the water supply and its components.</p> <p>Reference: <i>FEMA 386-7</i></p>	
5.4	<p><b>Does the building or site have storage capacity for domestic water?</b></p>	<p>Operational facilities will require reliance on adequate domestic water supply. Storage capacity can meet short-term needs and use water trucks to replenish for extended outages.</p>	

Table 1-22: Building Vulnerability Assessment Checklist\* (continued)

Section	Vulnerability Question	Guidance	Observations
	<b>How many gallons of storage capacity are available and how long will it allow operations to continue?</b>	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i> .	
5.5	<b>What is the source of water for the fire suppression system? (local utility company lines, storage tanks with utility company backup, lake, or river)</b>  <b>Are there alternate water supplies for fire suppression?</b>	The fire suppression system water may be supplied from the domestic water or it may have a separate source, separate storage, or nonpotable alternate sources.  For a site with multiple buildings, the concern is that the supply should be adequate to fight the worst case situation according to the fire codes. Recent major construction may change that requirement.  Reference: <i>FEMA 386-7</i>	
5.6	<b>Is the fire suppression system adequate, code-compliant, and protected (secure location)?</b>	Standpipes, water supply control valves, and other system components should be secure or supervised.  Reference: <i>FEMA 386-7</i>	
5.7	<b>Do the sprinkler/standpipe interior controls (risers) have fire- and blast-resistant separation?</b>  <b>Are the sprinkler and standpipe connections adequate and redundant?</b>  <b>Are there fire hydrant and water supply connections near the sprinkler/standpipe connections?</b>	The incoming fire protection water line should be encased, buried, or located 50 feet from high-risk areas. The interior mains should be looped and sectionalized.  Reference: <i>GSA PBS-P100</i>	
5.8	<b>Are there redundant fire water pumps (e.g., one electric, one diesel)?</b>  <b>Are the pumps located apart from each other?</b>	Collocating fire water pumps puts them at risk for a single incident to disable the fire suppression system.  References: <i>GSA PBS-P100 and FEMA 386-7</i>	
5.9	<b>Are sewer systems accessible?</b>  <b>Are they protected or secured?</b>	Sanitary and stormwater sewers should be protected from unauthorized access. The main concerns are backup or flooding into the building, causing a health risk, shorting out electrical equipment, and loss of building use.  Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
5.10	<b>What fuel supplies do the building rely upon for critical operation?</b>	Typically, natural gas, propane, or fuel oil are required for continued operation.  Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	

Table 1-22: Building Vulnerability Assessment Checklist\* (continued)

Section	Vulnerability Question	Guidance	Observations
5.11	<p><b>How much fuel is stored on the site or at the building and how long can this quantity support critical operations?</b></p> <p><b>How is it stored?</b></p> <p><b>How is it secured?</b></p>	<p>Fuel storage protection is essential for continued operation.</p> <p>Main fuel storage should be located away from loading docks, entrances, and parking. Access should be restricted and protected (e.g., locks on caps and seals).</p> <p>References: <i>GSA PBS-P100 and Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
5.12	<p><b>Where is the fuel supply obtained?</b></p> <p><b>How is it delivered?</b></p>	<p>The supply of fuel is dependent on the reliability of the supplier.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
5.13	<p><b>Are there alternate sources of fuel?</b></p> <p><b>Can alternate fuels be used?</b></p>	<p>Critical functions may be served by alternate methods if normal fuel supply is interrupted.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
5.14	<p><b>What is the normal source of electrical service for the site or building?</b></p>	<p>Utilities are the general source unless co-generation or a private energy provider is available.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
5.15	<p><b>Is there a redundant electrical service source?</b></p> <p><b>Can the site or buildings be fed from more than one utility substation?</b></p>	<p>The utility may have only one source of power from a single substation. There may be only single feeders from the main substation.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
5.16	<p><b>How many service entry points does the site or building have for electricity?</b></p>	<p>Electrical supply at one location creates a vulnerable situation unless an alternate source is available.</p> <p>Ensure disconnecting requirements according to NFPA 70 (National Fire Protection Association, National Electric Code) are met for multiple service entrances.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
5.17	<p><b>Is the incoming electric service to the building secure?</b></p>	<p>Typically, the service entrance is a locked room, inaccessible to the public.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	

Table 1-22: Building Vulnerability Assessment Checklist\* (continued)

Section	Vulnerability Question	Guidance	Observations
5.18	<p><b>What provisions for emergency power exist? What systems receive emergency power and have capacity requirements been tested?</b></p> <p><b>Is the emergency power collocated with the commercial electric service?</b></p> <p><b>Is there an exterior connection for emergency power?</b></p>	<p>Besides installed generators to supply emergency power, portable generators or rental generators available under emergency contract can be quickly connected to a building with an exterior quick disconnect already installed.</p> <p>Testing under actual loading and operational conditions ensures the critical systems requiring emergency power receive it with a high assurance of reliability.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
5.19	<p><b>By what means do the main telephone and data communications interface the site or building?</b></p>	<p>Typically, communication ducts or other conduits are available. Overhead service is more identifiable and vulnerable.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
5.20	<p><b>Are there multiple or redundant locations for the telephone and communications service?</b></p>	<p>Secure locations of communications wiring entry to the site or building are required.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
5.21	<p><b>Does the fire alarm system require communication with external sources?</b></p> <p><b>By what method is the alarm signal sent to the responding agency: telephone, radio, etc.?</b></p> <p><b>Is there an intermediary alarm monitoring center?</b></p>	<p>Typically, the local fire department responds to an alarm that sounds at the station or is transmitted over phone lines by an auto dialer.</p> <p>An intermediary control center for fire, security, and/or building system alarms may receive the initial notification at an on-site or off-site location. This center may then determine the necessary response and inform the responding agency.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
5.22	<p><b>Are utility lifelines aboveground, underground, or direct buried?</b></p>	<p>Utility lifelines (water, power, communications, etc.) can be protected by concealing, burying, or encasing.</p> <p>References: <i>GSA PBS-P100 and FEMA 386-7</i></p>	

Table 1-22: Building Vulnerability Assessment Checklist\* (continued)

Section	Vulnerability Question	Guidance	Observations
<b>6</b>	<b>Mechanical Systems (HVAC and CBR)</b>		
<b>6.1</b>	<p><b>Where are the air intakes and exhaust louvers for the building? (low, high, or midpoint of the building structure)</b></p> <p><b>Are the intakes and exhausts accessible to the public?</b></p>	<p>Air intakes should be located on the roof or as high as possible. Otherwise secure within CPTED-compliant fencing or enclosure. The fencing or enclosure should have a sloped roof to prevent the throwing of anything into the enclosure near the intakes.</p> <p>Reference: <i>GSA PBS-P100</i> states that air intakes should be on the fourth floor or higher and, on buildings with three floors or less, they should be on the roof or as high as practical. Locating intakes high on a wall is preferred over a roof location.</p> <p>Reference: <i>DoD UFC 4-010-01</i> states that, for all new inhabited buildings covered by this document, all air intakes should be located at least 3 meters (10 feet) above the ground.</p> <p>Reference: <i>CDC/NIOSH, Pub 2002-139</i> states: "An extension height of 12 feet (3.7 m) will place the intake out of reach of individuals without some assistance. Also, the entrance to the intake should be covered with a sloped metal mesh to reduce the threat of objects being tossed into the intake. A minimum slope of 45° is generally adequate. Extension height should be increased where existing platforms or building features (i.e., loading docks, retaining walls) might provide access to the outdoor air intakes".</p> <p>Reference: <i>LBNL PUB-51959</i>: Exhausts are also a concern during an outdoor release, especially if exhaust fans are not in continuous operation, due to wind effects and chimney effects (air movement due to differential temperature).</p>	
<b>6.2</b>	<p><b>Is roof access limited to authorized personnel by means of locking mechanisms?</b></p> <p><b>Is access to mechanical areas similarly controlled?</b></p>	<p>Roofs are like entrances to the building and are like mechanical rooms when HVAC is installed. Adjacent structures or landscaping should not allow access to the roof.</p> <p>References: <i>GSA PBS-P100, CDC/NIOSH Pub 2002-139, and LBNL Pub 51959</i></p>	
<b>6.3</b>	<b>Are there multiple air intake locations?</b>	<p>Single air intakes may feed several air handling units. Indicate if the air intakes are localized or separated. Installing low-leakage dampers is one way to provide the system separation when necessary.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
<b>6.4</b>	<b>What are the types of air filtration? Include the efficiency and number of filter modules for</b>	<p>MERV – Minimum Efficiency Reporting Value</p> <p>HEPA – High Efficiency Particulate Air</p>	

Table 1-22: Building Vulnerability Assessment Checklist\* (continued)

Section	Vulnerability Question	Guidance	Observations
	<p><b>each of the main air handling systems?</b></p> <p><b>Is there any collective protection for chemical, biological, and radiological contamination designed into the building?</b></p>	<p>Activated charcoal for gases</p> <p>Ultraviolet C for biologicals</p> <p>Consider mix of approaches for optimum protection and cost-effectiveness.</p> <p>Reference: <i>CDC/NIOSH Pub 2002-139</i></p>	
6.5	<b>Is there space for larger filter assemblies on critical air handling systems?</b>	<p>Air handling units serving critical functions during continued operation may be retrofitted to provide enhanced protection during emergencies. However, upgraded filtration may have negative effects upon the overall air handling system operation, such as increased pressure drop.</p> <p>Reference: <i>CDC/NIOSH Pub 2002-139</i></p>	
6.6	<b>Are there provisions for air monitors or sensors for chemical or biological agents?</b>	<p>Duct mounted sensors are usually found in limited cases in laboratory areas. Sensors generally have a limited spectrum of high reliability and are costly. Many different technologies are undergoing research to provide capability.</p> <p>Reference: <i>CDC/NIOSH Pub 2002-139</i></p>	
6.7	<b>By what method are air intakes and exhausts closed when not operational?</b>	<p>Motorized (low-leakage, fast-acting) dampers are the preferred method for closure with fail-safe to the closed position so as to support in-place sheltering.</p> <p>References: <i>CDC/NIOSH Pub 2002-139 and LBNL Pub 51959</i></p>	
6.8	<p><b>How are air handling systems zoned?</b></p> <p><b>What areas and functions do each of the primary air handling systems serve?</b></p>	<p>Understanding the critical areas of the building that must continue functioning focuses security and hazard mitigation measures.</p> <p>Applying HVAC zones that isolate lobbies, mailrooms, loading docks, and other entry and storage areas from the rest of the building HVAC zones and maintaining negative pressure within these areas will contain CBR releases. Identify common return systems that service more than one zone, effectively making a large single zone.</p> <p>Conversely, emergency egress routes should receive positive pressurization to ensure contamination does not hinder egress. Consider filtering of the pressurization air.</p> <p>References: <i>CDC/NIOSH Pub 2002-139 and LBNL Pub 51959</i></p>	
6.9	<b>Are there large central air handling units or are there multiple units serving separate zones?</b>	<p>Independent units can continue to operate if damage occurs to limited areas of the building.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	



Table 1-22: Building Vulnerability Assessment Checklist\* (continued)

Section	Vulnerability Question	Guidance	Observations
6.10	<p><b>Are there any redundancies in the air handling system?</b></p> <p><b>Can critical areas be served from other units if a major system is disabled?</b></p>	<p>Redundancy reduces the security measures required compared to a non-redundant situation.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
6.11	<p><b>Is the air supply to critical areas compartmentalized?</b></p> <p><b>Similarly, are the critical areas or the building as a whole, considered tight with little or no leakage?</b></p>	<p>During chemical, biological, and radiological situations, the intent is to either keep the contamination localized in the critical area or prevent its entry into other critical, non-critical, or public areas. Systems can be cross-connected through building openings (doorways, ceilings, partial wall), ductwork leakage, or pressure differences in air handling system. In standard practice, there is almost always some air carried between ventilation zones by pressure imbalances, due to elevator piston action, chimney effect, and wind effects.</p> <p>Smoke testing of the air supply to critical areas may be necessary.</p> <p>Reference: <i>CDC/NIOSH Pub 2002-139 and LBNL Pub 51959</i></p>	
6.12	<p><b>Are supply, return, and exhaust air systems for critical areas secure?</b></p> <p><b>Are all supply and return ducts completely connected to their grilles and registers and secure?</b></p> <p><b>Is the return air not ducted?</b></p>	<p>The air systems to critical areas should be inaccessible to the public, especially if the ductwork runs through the public areas of the building. It is also more secure to have a ducted air handling system versus sharing hallways and plenums above drop ceilings for return air. Non-ducted systems provide greater opportunity for introducing contaminants.</p> <p>Reference: <i>CDC/NIOSH Pub 2002-139 and LBNL Pub 51959</i></p>	
6.13	<p><b>What is the method of temperature and humidity control?</b></p> <p><b>Is it localized or centralized?</b></p>	<p>Central systems can range from monitoring only to full control. Local control may be available to override central operation.</p> <p>Of greatest concern are systems needed before, during, and after an incident that may be unavailable due to temperature and humidity exceeding operational limits (e.g., main telephone switch room).</p> <p>Reference: <i>DOC CIAO Vulnerability Assessment Framework 1.1</i></p>	
6.14	<p><b>Where are the building automation control centers and cabinets located?</b></p>	<p>Access to any component of the building automation and control system could compromise the functioning of the system, increasing vulnerability to a hazard or precluding their proper operation during a hazard incident.</p>	

Table 1-22: Building Vulnerability Assessment Checklist\* (continued)

Section	Vulnerability Question	Guidance	Observations
	<b>Are they in secure areas?</b> <b>How is the control wiring routed?</b>	<p>The HVAC and exhaust system controls should be in a secure area that allows rapid shutdown or other activation based upon location and type of attack.</p> <p>References: <i>FEMA 386-7, DOC CIAO Vulnerability Assessment Framework 1.1 and LBNL Pub 51959</i></p>	
6.15	<b>Does the control of air handling systems support plans for sheltering in place or other protective approach?</b>	<p>The micro-meteorological effects of buildings and terrain can alter travel and duration of chemical agents and hazardous material releases. Shielding in the form of sheltering in place can protect people and property from harmful effects.</p> <p>To support in-place sheltering, the air handling systems require the ability for authorized personnel to rapidly turn off all systems. However, if the system is properly filtered, then keeping the system operating will provide protection as long as the air handling system does not distribute an internal release to other portions of the building.</p> <p>Reference: <i>CDC/NIOSH Pub 2002-139</i></p>	
6.16	<b>Are there any smoke evacuation systems installed?</b> <b>Does it have purge capability?</b>	<p>For an internal blast, a smoke removal system may be essential, particularly in large, open spaces. The equipment should be located away from high-risk areas, the system controls and wiring should be protected, and it should be connected to emergency power. This exhaust capability can be built into areas with significant risk on internal events, such as lobbies, loading docks, and mailrooms. Consider filtering of the exhaust to capture CBR contaminants.</p> <p>References: <i>GSA PBS-P100, CDC/NIOSH Pub 2002-139, and LBNL Pub 51959</i></p>	
6.17	<b>Where is roof-mounted equipment located on the roof? (near perimeter, at center of roof)</b>	<p>Roof-mounted equipment should be kept away from the building perimeter.</p> <p>Reference: <i>U.S. Army TM 5-853</i></p>	
6.18	<b>Are fire dampers installed at all fire barriers?</b> <b>Are all dampers functional and seal well when closed?</b>	<p>All dampers (fire, smoke, outdoor air, return air, bypass) must be functional for proper protection within the building during an incident.</p> <p>Reference: <i>CDC/NIOSH Pub 2002-139</i></p>	
6.19	<b>Do fire walls and fire doors maintain their integrity?</b>	<p>The tightness of the building (both exterior, by weatherization to seal cracks around doors and windows, and internal, by zone ducting, fire walls, fire stops, and fire doors) provides energy conservation benefits and functional benefits during a CBR incident.</p> <p>Reference: <i>LBNL Pub 51959</i></p>	

Table 1-22: Building Vulnerability Assessment Checklist\* (continued)

Section	Vulnerability Question	Guidance	Observations
6.20	<b>Do elevators have recall capability and elevator emergency message capability?</b>	<p>Although a life-safety code and fire response requirement, the control of elevators also has benefit during a CBR incident. The elevators generate a piston effect, causing pressure differentials in the elevator shaft and associated floors that can force contamination to flow up or down.</p> <p>Reference: <i>LBNL Pub 51959</i></p>	
6.21	<b>Is access to building information restricted?</b>	<p>Information on building operations, schematics, procedures, plans, and specifications should be strictly controlled and available only to authorized personnel.</p> <p>References: <i>CDC/NIOSH Pub 2002-139 and LBNL Pub 51959</i></p>	
6.22	<b>Does the HVAC maintenance staff have the proper training, procedures, and preventive maintenance schedule to ensure CBR equipment is functional?</b>	<p>Functional equipment must interface with operational procedures in an emergency plan to ensure the equipment is properly operated to provide the protection desired.</p> <p>The HVAC system can be operated in different ways, depending upon an external or internal release and where in the building an internal release occurs. Thus maintenance and security staff must have the training to properly operate the HVAC system under different circumstances, even if the procedure is to turn off all air movement equipment.</p> <p>Reference: <i>CDC/NIOSH Pub 2002-139 and LBNL Pub 51959</i></p>	
<b>7 Plumbing and Gas Systems</b>			
7.1	<b>What is the method of water distribution?</b>	<p>Central shaft locations for piping are more vulnerable than multiple riser locations.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
7.2	<b>What is the method of gas distribution? (heating, cooking, medical, process)</b>	<p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
7.3	<b>Is there redundancy to the main piping distribution?</b>	<p>Looping of piping and use of section valves provide redundancies in the event sections of the system are damaged.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	

Table 1-22: Building Vulnerability Assessment Checklist\* (continued)

Section	Vulnerability Question	Guidance	Observations
7.4	<b>What is the method of heating domestic water?</b> <b>What fuel(s) is used?</b>	<p>Single source of hot water with one fuel source is more vulnerable than multiple sources and multiple fuel types. Domestic hot water availability is an operational concern for many building occupancies.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
7.5	<b>Where are gas storage tanks located? (heating, cooking, medical, process)</b> <b>How are they piped to the distribution system? (above or below ground)</b>	<p>The concern is that the tanks and piping could be vulnerable to a moving vehicle or a bomb blast either directly or by collateral damage due to proximity to a higher-risk area.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
7.6	<b>Are there reserve supplies of critical gases?</b>	<p>Localized gas cylinders could be available in the event of damage to the central tank system.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
<b>8 Electrical Systems</b>			
8.1	<b>Are there any transformers or switchgears located outside the building or accessible from the building exterior?</b> <b>Are they vulnerable to public access?</b> <b>Are they secured?</b>	<p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
8.2	<b>What is the extent of the external building lighting in utility and service areas and at normal entryways used by the building occupants?</b>	<p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
8.3	<b>How are the electrical rooms secured and where are they located relative to other higher-risk areas, starting with the main electrical distribution room at the service entrance?</b>	<p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	

Table 1-22: Building Vulnerability Assessment Checklist\* (continued)

Section	Vulnerability Question	Guidance	Observations
8.4	<p><b>Are critical electrical systems collocated with other building systems?</b></p> <p><b>Are critical electrical systems located in areas outside of secured electrical areas?</b></p> <p><b>Is security system wiring located separately from electrical and other service systems?</b></p>	<p>Collocation concerns include rooms, ceilings, raceways, conduits, panels, and risers.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
8.5	<p><b>How are electrical distribution panels serving branch circuits secured or are they in secure locations?</b></p>	<p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
8.6	<p><b>Does emergency backup power exist for all areas within the building or for critical areas only?</b></p> <p><b>How is the emergency power distributed?</b></p> <p><b>Is the emergency power system independent from the normal electrical service, particularly in critical areas?</b></p>	<p>There should be no single critical node that allows both the normal electrical service and the emergency backup power to be affected by a single incident. Automatic transfer switches and interconnecting switchgear are the initial concerns.</p> <p>Emergency and normal electrical equipment should be installed separately, at different locations, and as far apart as possible.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
8.7	<p><b>How is the primary electrical system wiring distributed?</b></p> <p><b>Is it collocated with other major utilities?</b></p> <p><b>Is there redundancy of distribution to critical areas?</b></p>	<p>Central utility shafts may be subject to damage, especially if there is only one for the building.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	

Table 1-22: Building Vulnerability Assessment Checklist\* (continued)

Section	Vulnerability Question	Guidance	Observations
<b>9 Fire Alarm Systems</b>			
9.1	<p><b>Is the building fire alarm system centralized or localized?</b></p> <p><b>How are alarms made known, both locally and centrally?</b></p> <p><b>Are critical documents and control systems located in a secure yet accessible location?</b></p>	<p>Fire alarm systems must first warn building occupants to evacuate for life safety. Then they must inform the responding agency to dispatch fire equipment and personnel.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
9.2	<p><b>Where are the fire alarm panels located?</b></p> <p><b>Do they allow access to unauthorized personnel?</b></p>	<p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
9.3	<p><b>Is the fire alarm system standalone or integrated with other functions such as security and environmental or building management systems?</b></p> <p><b>What is the interface?</b></p>	<p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
9.4	<p><b>Do key fire alarm system components have fire- and blast-resistant separation?</b></p>	<p>This is especially necessary for the fire command center or fire alarm control center. The concern is to similarly protect critical components as described in Items 2.19, 5.7, and 10.3.</p>	
9.5	<p><b>Is there redundant off-premises fire alarm reporting?</b></p>	<p>Fire alarms can ring at a fire station, at an intermediary alarm monitoring center, or autodial someone else. See Items 5.21 and 10.5.</p>	
<b>10 Communications and IT Systems</b>			
10.1	<p><b>Where is the main telephone distribution room and where is it in relation to higher-risk areas?</b></p> <p><b>Is the main telephone distribution room secure?</b></p>	<p>One can expect to find voice, data, signal, and alarm systems to be routed through the main telephone distribution room.</p> <p>Reference: <i>FEMA 386-7</i></p>	

Table 1-22: Building Vulnerability Assessment Checklist\* (continued)

Section	Vulnerability Question	Guidance	Observations
10.2	<p><b>Does the telephone system have an uninterruptible power supply (UPS)?</b></p> <p><b>What is its type, power rating, and operational duration under load, and location? (battery, on-line, filtered)</b></p>	<p>Many telephone systems are now computerized and need a UPS to ensure reliability during power fluctuations. The UPS is also needed to await any emergency power coming on line or allow orderly shutdown.</p> <p>Reference: <i>DOC CIAO Vulnerability Assessment Framework 1.1</i></p>	
10.3	<p><b>Where are communication systems wiring closets located? (voice, data, signal, alarm)</b></p> <p><b>Are they collocated with other utilities?</b></p> <p><b>Are they in secure areas?</b></p>	<p>Concern is to have separation distance from other utilities and higher-risk areas to avoid collateral damage.</p> <p>Security approaches on the closets include door alarms, closed circuit television, swipe cards, or other logging notifications to ensure only authorized personnel have access to these closets.</p> <p>Reference: <i>FEMA 386-7</i></p>	
10.4	<p><b>How is the communications system wiring distributed? (secure chases and risers, accessible public areas)</b></p>	<p>The intent is to prevent tampering with the systems.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
10.5	<p><b>Are there redundant communications systems available?</b></p>	<p>Critical areas should be supplied with multiple or redundant means of communications. Power outage phones can provide redundancy as they connect directly to the local commercial telephone switch off site and not through the building telephone switch in the main telephone distribution room.</p> <p>A base radio communication system with antenna can be installed in stairwells, and portable sets distributed to floors.</p> <p>References: <i>GSA PBS-P100 and FEMA 386-7</i></p>	
10.6	<p><b>Where are the main distribution facility, data centers, routers, firewalls, and servers located and are they secure?</b></p> <p><b>Where are the secondary and/or intermediate distribution facilities and are they secure?</b></p>	<p>Concern is collateral damage from manmade hazards and redundancy of critical functions.</p> <p>Reference: <i>DOC CIAO Vulnerability Assessment Framework 1.1</i></p>	
10.7	<p><b>What type and where are the Wide Area Network (WAN) connections?</b></p>	<p>Critical facilities should have two Minimum-Points-of-Presence( MPOPs) where the telephone company's outside cable terminates inside the building. It is functionally a service entrance connection that demarcates where the telephone company's property stops and the building owner's property begins. The MPOPs should not be</p>	

Table 1-22: Building Vulnerability Assessment Checklist\* (continued)

Section	Vulnerability Question	Guidance	Observations
		<p>collocated and they should connect to different telephone company central offices so that the loss of one cable or central office does not reduce capability.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
10.8	<p><b>What are the type, power rating, and location of the uninterruptible power supply?</b> (battery, on-line, filtered)</p> <p><b>Are the UPS also connected to emergency power?</b></p>	<p>Consider that UPS should be found at all computerized points from the main distribution facility to individual data closets and at critical personal computers/terminals.</p> <p>Critical LAN sections should also be on backup power.</p> <p>Reference: <i>DOC CIAO Vulnerability Assessment Framework 1.1</i></p>	
10.9	<p><b>What type of Local Area Network (LAN) cabling and physical topology is used?</b> (Category (Cat) 5, Gigabit Ethernet, Ethernet, Token Ring)</p>	<p>The physical topology of a network is the way in which the cables and computers are connected to each other. The main types of physical topologies are:</p> <p>Bus (single radial where any damage on the bus affects the whole system, but especially all portions downstream)</p> <p>Star (several computes are connected to a hub and many hubs can be in the network – the hubs can be critical nodes, but the other hubs continue to function if one fails)</p> <p>Ring (a bus with a continuous connection - least used, but can tolerate some damage because if the ring fails at a single point it can be rerouted much like a looped electric or water system)</p> <p>The configuration and the availability of surplus cable or spare capacity on individual cables can reduce vulnerability to hazard incidents.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
10.10	<p><b>For installed radio/wireless systems, what are their types and where are they located?</b> (radio frequency (RF), high frequency (HF), very high frequency (VHF), medium wave (MW))</p>	<p>Depending upon the function of the wireless system, it could be susceptible to accidental or intended jamming or collateral damage.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
10.11	<p><b>Do the Information Technology (IT - computer) systems meet requirements of confidentiality, integrity, and availability?</b></p>	<p>Ensure access to terminals and equipment for authorized personnel only and ensure system up-time to meet operational needs.</p> <p>Reference: <i>DOC CIAO Vulnerability Assessment Framework 1.1</i></p>	



Table 1-22: Building Vulnerability Assessment Checklist\* (continued)

Section	Vulnerability Question	Guidance	Observations
10.12	<b>Where is the disaster recovery/ mirroring site?</b>	A site with suitable equipment that allows continuation of operations or that mirrors (operates in parallel to) the existing operation is beneficial if equipment is lost during a natural or manmade disaster. The need is based upon the criticality of the operation and how quickly replacement equipment can be put in place and operated.  Reference: <i>DOC CIAO Vulnerability Assessment Framework 1.1</i>	
10.13	<b>Where is the backup tape/file storage site and what is the type of safe environment?</b> (safe, vault, underground)  <b>Is there redundant refrigeration in the site?</b>	If equipment is lost, data are most likely lost, too. Backups are needed to continue operations at the disaster recovery site or when equipment can be delivered and installed.  Reference: <i>DOC CIAO Vulnerability Assessment Framework 1.1</i>	
10.14	<b>Are there any satellite communications (SATCOM) links?</b> (location, power, UPS, emergency power, spare capacity/capability)	SATCOM links can serve as redundant communications for voice and data if configured to support required capability after a hazard incident.  Reference: <i>DOC CIAO Vulnerability Assessment Framework 1.1</i>	
10.15	<b>Is there a mass notification system that reaches all building occupants?</b> (public address, pager, cell phone, computer override, etc.)  <b>Will one or more of these systems be operational under hazard conditions?</b> (UPS, emergency power)	Depending upon building size, a mass notification system will provide warning and alert information, along with actions to take before and after an incident if there is redundancy and power.  Reference: <i>DoD UFC 4-010-01</i>	
10.16	<b>Do control centers and their designated alternate locations have equivalent or reduced capability for voice, data, mass notification, etc.?</b> (emergency operations, security, fire alarms, building automation)  <b>Do the alternate locations also have access to backup systems, including emergency power?</b>	Reference: <i>GSA PBS-P100</i>	

Table 1-22: Building Vulnerability Assessment Checklist\* (continued)

Section	Vulnerability Question	Guidance	Observations
<b>11</b>	<b>Equipment Operations and Maintenance</b>		
<b>11.1</b>	<p><b>Are there composite drawings indicating location and capacities of major systems and are they current?</b> (electrical, mechanical, and fire protection; and date of last update)</p> <p><b>Do updated operations and maintenance (O&amp;M) manuals exist?</b></p>	<p>Within critical infrastructure protection at the building level, the current configuration and capacity of all critical systems must be understood to ensure they meet emergency needs. Manuals must also be current to ensure operations and maintenance keeps these systems properly functioning. The system must function during an emergency unless directly affected by the hazard incident.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
<b>11.2</b>	<p><b>Have critical air systems been rebalanced?</b></p> <p><b>If so, when and how often?</b></p>	<p>Although the system may function, it must be tested periodically to ensure it is performing as designed. Balancing is also critical after initial construction to set equipment to proper performance per the design.</p> <p>Rebalancing may only occur during renovation.</p> <p>Reference: <i>CDC/NIOSH Pub 2002-139</i></p>	
<b>11.3</b>	<b>Is air pressurization monitored regularly?</b>	<p>Some areas require positive or negative pressure to function properly. Pressurization is critical in a hazardous environment or emergency situation.</p> <p>Measuring pressure drop across filters is an indication when filters should be changed, but also may indicate that low pressures are developing downstream and could result in loss of expected protection.</p> <p>Reference: <i>CDC/NIOSH Pub 2002-139</i></p>	
<b>11.4</b>	<b>Does the building have a policy or procedure for periodic recommissioning of major Mechanical/Electrical/Plumbing (M/E/P) systems?</b>	<p>Recommissioning involves testing and balancing of systems to ascertain their capability to perform as described.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
<b>11.5</b>	<b>Is there an adequate O&amp;M program, including training of facilities management staff?</b>	<p>If O&amp;M of critical systems is done with in-house personnel, management must know what needs to be done and the workforce must have the necessary training to ensure systems reliability.</p> <p>Reference: <i>CDC/NIOSH Pub 2002-139</i></p>	
<b>11.6</b>	<b>What maintenance and service agreements exist for M/E/P systems?</b>	<p>When an in-house facility maintenance work force does not exist or does not have the capability to perform the work, maintenance and service contracts are the alternative to ensure critical systems will work under all</p>	

Table 1-22: Building Vulnerability Assessment Checklist\* (continued)

Section	Vulnerability Question	Guidance	Observations
		<p>conditions. The facility management staff requires the same knowledge to oversee these contracts as if the work was being done by in-house personnel.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
11.7	<b>Are backup power systems periodically tested under load?</b>	<p>Loading should be at or above maximum connected load to ensure available capacity and automatic sensors should be tested at least once per year.</p> <p>Periodically (once a year as a minimum) check the duration of capacity of backup systems by running them for the expected emergency duration or estimating operational duration through fuel consumption, water consumption, or voltage loss.</p> <p>Reference: <i>FEMA 386-7</i></p>	
11.8	<b>Is stairway and exit sign lighting operational?</b>	<p>The maintenance program for stairway and exit sign lighting (all egress lighting) should ensure functioning under normal and emergency power conditions.</p> <p>Expect building codes to be updated as emergency egress lighting is moved from upper walls and over doorways to floor level as heat and smoke drive occupants to crawl along the floor to get out of the building. Signs and lights mounted high have limited or no benefit when obscured.</p> <p>Reference: <i>FEMA 386-7</i></p>	
<b>12 Security Systems</b>			
Perimeter Systems			
12.1	<p><b>Are black/white or color CCTV (closed circuit television) cameras used?</b></p> <p><b>Are they monitored and recorded 24 hours/7 days a week? By whom?</b></p> <p><b>Are they analog or digital by design?</b></p> <p><b>What are the number of fixed, wireless, and pan-tilt-zoom cameras used?</b></p>	<p>Security technology is frequently considered to complement or supplement security personnel forces and to provide a wider area of coverage. Typically, these physical security elements provide the first line of defense in deterring, detecting, and responding to threats and reducing vulnerabilities. They must be viewed as an integral component of the overall security program. Their design, engineering, installation, operation, and management must be able to meet daily security challenges from a cost-effective and efficiency perspective. During and after an incident, the system, or its backups, should be functional per the planned design.</p> <p>Consider color CCTV cameras to view and record activity at the perimeter of the building, particularly at primary entrances and exits. A mix of monochrome cameras</p>	

Table 1-22: Building Vulnerability Assessment Checklist\* (continued)

Section	Vulnerability Question	Guidance	Observations
	<p><b>Who are the manufacturers of the CCTV cameras?</b></p> <p><b>What is the age of the CCTV cameras in use?</b></p>	<p>should be considered for areas that lack adequate illumination for color cameras.</p> <p>Reference: <i>GSA PBS P-100</i></p>	
12.2	<p><b>Are the cameras programmed to respond automatically to perimeter building alarm events?</b></p> <p><b>Do they have built-in video motion capabilities?</b></p>	<p>The efficiency of monitoring multiple screens decreases as the number of screens increases. Tying the alarm system or motion sensors to a CCTV camera and a monitoring screen improves the man-machine interface by drawing attention to a specific screen and its associated camera. Adjustment may be required after installation due to initial false alarms, usually caused by wind or small animals.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
12.3	<p><b>What type of camera housings are used and are they environmental in design to protect against exposure to heat and cold weather elements?</b></p>	<p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
12.4	<p><b>Are panic/duress alarm buttons or sensors used, where are they located, and are they hardwired or portable?</b></p>	<p>Call buttons should be provided at key public contact areas and as needed in offices of managers and directors, in garages and parking lots, and other high-risk locations by assessment.</p> <p>Reference: <i>GSA PBS P-100</i></p>	
12.5	<p><b>Are intercom call boxes used in parking areas or along the building perimeter?</b></p>	<p>See Item 12.4.</p>	
12.6	<p><b>What is the transmission media used to transmit camera video signals: fiber, wire line, telephone wire, coaxial, wireless?</b></p>	<p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
12.7	<p><b>Who monitors the CCTV system?</b></p>	<p>Reference: <i>DOC CIAO Vulnerability Assessment Framework 1.1</i></p>	

Table 1-22: Building Vulnerability Assessment Checklist\* (continued)

Section	Vulnerability Question	Guidance	Observations
12.8	<p><b>What is the quality of video images both during the day and hours of darkness?</b></p> <p><b>Are infrared camera illuminators used?</b></p>	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
12.9	<p><b>Are the perimeter cameras supported by an uninterruptible power supply, battery, or building emergency power?</b></p>	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
12.10	<p><b>What type of exterior Intrusion Detection System (IDS) sensors are used?</b> (electromagnetic; fiber optic; active infrared; bistatic microwave; seismic; photoelectric; ground; fence; glass break (vibration/shock); single, double, and roll-up door magnetic contacts or switches)</p>	<p>Consider balanced magnetic contact switch sets for all exterior doors, including overhead/roll-up doors, and review roof intrusion detection.</p> <p>Consider glass break sensors for windows up to scalable heights.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
12.11	<p><b>Is a global positioning system (GPS) used to monitor vehicles and asset movements?</b></p>	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
Interior Security			
12.12	<p><b>Are black/white or color CCTV cameras used?</b></p> <p><b>Are they monitored and recorded 24 hours/7 days a week? By whom?</b></p> <p><b>Are they analog or digital by design?</b></p> <p><b>What are the number of fixed, wireless, and pan-tilt-zoom cameras used?</b></p> <p><b>Who are the manufacturers of the CCTV cameras?</b></p> <p><b>What is the age of the CCTV cameras in use?</b></p>	<p>See Item 12.1.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	

Table 1-22: Building Vulnerability Assessment Checklist\* (continued)

Section	Vulnerability Question	Guidance	Observations
12.13	<p><b>Are the cameras programmed to respond automatically to interior building alarm events?</b></p> <p><b>Do they have built-in video motion capabilities?</b></p>	<p>The efficiency of monitoring multiple screens decreases as the number of screens increases. Tying the alarm system or motion sensors to a CCTV camera and a monitoring screen improves the man-machine interface by drawing attention to a specific screen and its associated camera.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
12.14	<b>What type of camera housings are used and are they designed to protect against exposure or tampering?</b>	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
12.15	<b>Do the camera lenses used have the proper specifications, especially distance viewing and clarity?</b>	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
12.16	<b>What is the transmission media used to transmit camera video signals: fiber, wire line, telephone wire, coaxial, wireless?</b>	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
12.17	<b>Are the interior camera video images of good visual and recording quality?</b>	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
12.18	<b>Are the interior cameras supported by an uninterruptible power supply source, battery, or building emergency power?</b>	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
12.19	<b>What are the first costs and maintenance costs associated with the interior cameras?</b>	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
12.20	<b>What type of security access control system is used?</b>	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	

Table 1-22: Building Vulnerability Assessment Checklist\* (continued)

Section	Vulnerability Question	Guidance	Observations
	<b>Are the devices used for physical security also used (integrated) with security computer networks (e.g., in place of or in combination with user ID and system passwords)?</b>		
12.21	<b>What type of access control transmission media is used to transmit access control system signals (same as defined for CCTV cameras)?</b>	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
12.22	<b>What is the backup power supply source for the access control systems? (battery, uninterruptible power supply)</b>	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
12.23	<b>What access control system equipment is used?</b>  <b>How old are the systems and what are the related first and maintenance service costs?</b>	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
12.24	<b>Are panic/duress alarm sensors used?</b>  <b>Where are they located?</b>  <b>Are they hardwired or portable?</b>	Call buttons should be provided at key public contact areas and as needed in offices of managers and directors, in garages and parking lots, and other high-risk locations by assessment.  Reference: <i>GSA PBS P-100</i>	
12.25	<b>Are intercom call-boxes or a building intercom system used throughout the building?</b>	See Item 12.24.	
12.26	<b>Are magnetometers (metal detectors) and x-ray equipment used?</b>  <b>At what locations within the building?</b>	Reference: <i>DOC CIAO Vulnerability Assessment Framework 1.1</i>	

Table 1-22: Building Vulnerability Assessment Checklist\* (continued)

Section	Vulnerability Question	Guidance	Observations
12.27	<b>What type of interior IDS sensors are used: electromagnetic; fiber optic; active infrared-motion detector; photoelectric; glass break (vibration/shock); single, double, and roll-up door magnetic contacts or switches?</b>	Consider magnetic reed switches for interior doors and openings.  Reference: <i>GSA PBS-P100</i>	
12.28	<b>Are mechanical, electrical, gas, power supply, radiological material storage, voice/data telecommunication system nodes, security system panels, elevator and critical system panels, and other sensitive rooms continuously locked, under electronic security, CCTV camera, and intrusion alarm systems surveillance?</b>	Reference: <i>DOC CIAO Vulnerability Assessment Framework 1.1</i>	
12.29	<b>What types of locking hardware are used throughout the building?</b>  <b>Are manual and electromagnetic cipher, keypad, pushbutton, panic bar, door strikes, and related hardware and software used?</b>	As a minimum, electric utility closets, mechanical rooms, and telephone closets should be secured.  The mailroom should also be secured, allowing only authorized personnel into the area where mail is screened and sorted. Separate the public access area from the screening area for the postulated mailroom threats.  All security locking arrangements on doors used for egress must comply with <i>NFPA 101, Life Safety Code</i> .  Reference: <i>GSA PBS-P100</i>	
12.30	<b>Are any potentially hazardous chemicals, combustible, or toxic materials stored on site in non-secure and non-monitored areas?</b>	The storage, use, and handling locations should also be kept away from other activities.  The concern is that an intruder need not bring the material into the building if it is already there and accessible.  Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
12.31	<b>What security controls are in place to handle the processing of mail and protect against potential biological, explosive, or other threatening exposures?</b>	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	



Table 1-22: Building Vulnerability Assessment Checklist\* (continued)

Section	Vulnerability Question	Guidance	Observations
12.32	<p><b>Is there a designated security control room and console in place to monitor security, fire alarm, and other building systems?</b></p> <p><b>Is there a backup control center designated and equipped?</b></p> <p><b>Is there off-site 24-hour monitoring of intrusion detection systems?</b></p>	<p>Monitoring can be done at an off-site facility, at an on-site monitoring center during normal duty hours, or at a 24-hour on-site monitoring center.</p> <p>Reference: <i>GSA PBS-P100</i></p>	
12.33	<p><b>Is the security console and control room adequate in size and does it provide room for expansion?</b></p> <p><b>Does it have adequate environment controls (e.g., a/c, lighting, heating, air circulation, backup power)?</b></p> <p><b>Is it ergonomically designed?</b></p>	<p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
12.34	<p><b>Is the location of the security room in a secure area with limited, controlled, and restricted access controls in place?</b></p>	<p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
12.35	<p><b>What are the means by which facility and security personnel can communicate with one another (e.g., portable radio, pager, cell phone, personal data assistants (PDAs))?</b></p> <p><b>What problems have been experienced with these and other electronic security systems?</b></p>	<p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
12.36	<p><b>Is there a computerized security incident reporting system used to prepare reports and track security incident trends and patterns?</b></p>	<p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
12.37	<p><b>Does the current security force have access to a computerized guard tour system?</b></p>	<p>This system allows for the systematic performance of guard patrols with validation indicators built in. The system notes stations/locations checked or missed, dates</p>	

Table 1-22: Building Vulnerability Assessment Checklist\* (continued)

Section	Vulnerability Question	Guidance	Observations
		<p>and times of such patrols, and who conducted them on what shifts. Management reports can be produced for recordkeeping and manpower analysis purposes.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
12.38	<p><b>Are vaults or safes in the building?</b></p> <p><b>Where are they located?</b></p>	<p>Basic structural design requires an understanding of where heavy concentrations of floor loading may occur so as to strengthen the floor and structural framing to handle this downward load. Security design also needs this information to analyze how this concentrated load affects upward and downward loadings under blast conditions and its impact upon progressive collapse. Location is important because safes can be moved by blast so that they should be located away from people and away from exterior windows.</p> <p>Vaults, on the other hand, require construction above the building requirements with thick masonry walls and steel reinforcement. A vault can provide protection in many instances due to its robust construction.</p> <p>Safes and vaults may also require security sensors and equipment, depending upon the level of protection and defensive layers needed.</p> <p>Reference: <i>U.S. Army TM 5-85</i></p>	
Security System Documents			
12.39	<b>Have security system as-built drawings been generated and are they ready for review?</b>	<p>Drawings are critical to the consideration and operation of security technologies, including its overall design and engineering processes. These historical reference documents outline system specifications and layout security devices used, as well as their application, location, and connectivity. They are a critical resource tool for troubleshooting system problems, and replacing and adding other security system hardware and software products. Such documents are an integral component to new and retrofit construction projects.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
12.40	<b>Have security system design and drawing standards been developed?</b>	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
12.41	<b>Are security equipment selection criteria defined?</b>	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	

Table 1-22: Building Vulnerability Assessment Checklist\* (continued)

Section	Vulnerability Question	Guidance	Observations
12.42	<b>What contingency plans have been developed or are in place to deal with security control center redundancy and backup operations?</b>	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
12.43	<b>Have security system construction specification documents been prepared and standardized?</b>	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
12.44	<b>Do all security system documents include current as-built drawings?</b>	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
12.45	<b>Have qualifications been determined for security consultants, system designers/ engineers, installation vendors, and contractors?</b>	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
12.46	<b>Are security systems decentralized, centralized, or integrated?</b>  <b>Do they operate over an existing IT network or are they a standalone method of operation?</b>	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
12.47	<b>What security systems manuals are available?</b>	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
12.48	<b>What maintenance or service agreements exist for security systems?</b>	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	

Table 1-22: Building Vulnerability Assessment Checklist\* (continued)

Section	Vulnerability Question	Guidance	Observations
<b>13</b>	<b>Security Master Plan</b>		
<b>13.1</b>	<p><b>Does a written security plan exist for this site or building?</b></p> <p><b>When was the initial security plan written and last revised?</b></p> <p><b>Who is responsible for preparing and reviewing the security plan?</b></p>	<p>The development and implementation of a security master plan provides a roadmap that outlines the strategic direction and vision, operational, managerial, and technological mission, goals, and objectives of the organization's security program.</p> <p>Reference: <i>DOC CIAO Vulnerability Assessment Framework 1.1</i></p>	
<b>13.2</b>	<b>Has the security plan been communicated and disseminated to key management personnel and departments?</b>	<p>The security plan should be part of the building design so that the construction or renovation of the structure integrates with the security procedures to be used during daily operations.</p> <p>Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i></p>	
<b>13.3</b>	<b>Has the security plan been benchmarked or compared against related organizations and operational entities?</b>	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
<b>13.4</b>	<b>Has the security plan ever been tested and evaluated from a benefit/cost and operational efficiency and effectiveness perspective?</b>	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
<b>13.5</b>	<b>Does the security plan define mission, vision, and short- and long- term security program goals and objectives?</b>	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
<b>13.6</b>	<b>Are threats/hazards, vulnerabilities, and risks adequately defined and security countermeasures addressed and prioritized relevant to their criticality and probability of occurrence?</b>	Reference: <i>DOC CIAO Vulnerability Assessment Framework 1.1</i>	
<b>13.7</b>	<b>Has a security implementation schedule been established to address recommended security solutions?</b>	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	

Table 1-22: Building Vulnerability Assessment Checklist\* (continued)

Section	Vulnerability Question	Guidance	Observations
13.8	Have security operating and capital budgets been addressed, approved, and established to support the plan?	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
13.9	What regulatory or industry guidelines/standards were followed in the preparation of the security plan?	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
13.10	Does the security plan address existing security conditions from an administrative, operational, managerial, and technical security systems perspective?	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
13.11	Does the security plan address the protection of people, property, assets, and information?	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
13.12	Does the security plan address the following major components: access control, surveillance, response, building hardening, and protection against CBR and cyber-network attacks?	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
13.13	Has the level of risk been identified and communicated in the security plan through the performance of a physical security assessment?	Reference: <i>Physical Security Assessment for the Department of Veterans Affairs Facilities</i>	
13.14	When was the last security assessment performed?  Who performed the security risk assessment?	Reference: <i>DOC CIAO Vulnerability Assessment Framework 1.1</i>	

Table 1-22: Building Vulnerability Assessment Checklist\* (continued)

Section	Vulnerability Question	Guidance	Observations
13.15	<p><b>Are the following areas of security analysis addressed in the security master plan?</b></p> <p><b>Asset Analysis:</b> Does the security plan identify and prioritize the assets to be protected in accordance to their location, control, current value, and replacement value?</p> <p><b>Threat Analysis:</b> Does the security plan address potential threats; causes of potential harm in the form of death, injury, destruction, disclosure, interruption of operations, or denial of services? (possible criminal acts [documented and review of police/security incident reports] associated with forced entry, bombs, ballistic assault, biochemical and related terrorist tactics, attacks against utility systems infrastructure and buildings)</p> <p><b>Vulnerability Analysis:</b> Does the security plan address other areas associated with the site or building and its operations that can be taken advantage of to carry out a threat? (architectural design and construction of new and existing buildings, technological support systems [e.g., heating, air conditioning, power, lighting and security systems, etc.] and operational procedures, policies, and controls)</p> <p><b>Risk Analysis:</b> Does the security plan address the findings from the asset, threat/hazard, and vulnerability analyses in order to develop, recommend, and consider implementation of appropriate security countermeasures?</p>	<p>This process is the input to the building design and what mitigation measures will be included in the facility project to reduce risk and increase safety of the building and people.</p> <p>Reference: <i>USA TM 5-853, Security Engineering</i></p>	

Table 1-22: Building Vulnerability Assessment Checklist\* (continued)

<b>*Sources:</b>
<p><b>Centers for Disease Control and Prevention/National Institute for Occupational Safety and Health (CDC/NIOSH)</b>  Publication No. 2002-139, <i>Guidance for Protecting Building Environments from Airborne Chemical, Biological, or Radiological Attacks</i>, May 2002</p>
<p><b>Federal Emergency Management Agency (FEMA)</b>  FEMA 154, <i>Rapid Visual Screening of Buildings for Seismic Hazards: A Handbook</i>, 1988 (also, Applied Technology Council (ATC-21) by same name)  FEMA 386-7, <i>Integrating Human-Caused Hazards Into Mitigation Planning</i>, September 2002  SLG 101, <i>Guide for All-Hazard Emergency Operations Planning</i>, Chapter 6, Attachment G, Terrorism, April 2001</p>
<p><b>General Services Administration (GSA)</b>  PBS – P100, <i>Facilities Standards for Public Buildings Service</i>, November 2002</p>
<p><b>Lawrence Berkeley National Laboratory (LBNL)</b>  LBNL PUB-51959, <i>Protecting Buildings from a Biological or Chemical Attack: Actions to Take Before or During a Release</i>, January 10, 2003</p>
<p><b>U.S. Air Force (USAF)</b>  <i>Installation Force Protection Guide</i>, 1997</p>
<p><b>U.S. Army (USA)</b>  Technical Manuals (TM) 5-853-1/-2/-3/-4, <i>Security Engineering</i>, May 12, 1994</p>
<p><b>U.S. Department of Commerce, Critical Infrastructure Assurance Office (DOC CIAO)</b>  <i>Vulnerability Assessment Framework 1.1</i>, October 1998</p>
<p><b>U.S. Department of Defense (DoD)</b>  Unified Facilities Criteria (UFC), UFC 4-010-01, <i>DoD Minimum Antiterrorism Standards for Buildings</i>, July 31, 2002</p>
<p><b>U.S. Department of Justice (DOJ)</b>  National Criminal Justice (NCJ) NCJ181200, <i>Fiscal Year 1999 State Domestic Preparedness Equipment Program, Assessment and Strategy Development Tool Kit</i>, May 15, 2000</p>
<p><b>U.S. Department of Veterans Affairs (VA)</b>  Physical Security Assessment for the Department of Veterans Affairs Facilities, <i>Recommendations of the National Institute of Building Sciences Task Group to the Department of Veterans Affairs</i>, 6 September 2002</p>





**T**his chapter discusses site-level considerations for development. The intent of this guidance is to provide concepts for integrating land use planning, landscape architecture (vegetation, landforms, and water), site planning, and other strategies to mitigate the design basis threats as identified via the risk assessment. Integrating security requirements into a larger, more comprehensive approach necessitates achieving a balance among many objectives such as reducing risk; facilitating proper building function; aesthetics and matching architecture; hardening of physical structures beyond required building codes and standards; and maximizing use of non-structural systems.

The design community must work closely with building owners and operators to ensure that the optimal balance of all the above considerations is achieved; thus, coordination within the design team is critical. Many asset protection objectives can be achieved during the early stages of the design process when mitigation is the least costly and most easily implemented. Planners, architects, and landscape designers play an important role in identifying and implementing crucial asset protection measures while considering land use; site selection; the orientation of buildings on the site; and the integration of vehicle access, control points, physical barriers, landscaping, parking, and protection of utilities to mitigate threats.

It is important to remember that the nature of any threat is always changing. Although indications of potential threats may be scarce during the design stage, consideration should be given to accommodating enhanced protection measures in response to future threats that may emerge. Asset protection objectives must be balanced with other design objectives, such as the efficient use of land and resources, and must also take into account existing physical, programmatic, and fiscal constraints.

## 2.1 LAND USE CONSIDERATIONS

Managing the many dimensions of land use (e.g., development, transportation, activities, and growth, etc.) is a well-established practice in the United States, with numerous regulations and other tools in use by state and local governments to influence the urban form. These tools range from private controls (e.g., deed restrictions and easements) to governmental mechanisms, including permitting, subdivision, land development regulations, and zoning. In addition, economic forces such as land market values, enterprise zones, insurance costs, tax incentives, and impact fees are major considerations in land use decision-making.

Many of these land use controls are significant factors of anti-terrorism and security. For example, zoning, subdivisions, and planned unit developments define urban configurations, which translate directly into potential terrorist attack opportunities because they provide protective clustering of some activities and defensive dispersion of others. Furthermore, performance-based zoning (in contrast to prescriptive zoning) can allow for greater freedom in land use by removing location-based use constraints in favor of simply assigning responsibility for any negative impacts directly to the land owner. The benefits of increased performance-based zoning's flexibility relies on the ability of the owner and/or operator to make informed decisions about the level of risk that they are willing to accept and how much risk they can mitigate through land use countermeasures.

As another example, a deed restriction limiting the use of an adjacent parcel to open space or recreation may present a security advantage in terms of setback, but such spaces may also make hostile surveillance and attack preparations difficult to detect or to discern from those of normal use. Impact fees on stormwater infrastructure may provide an economic incentive to implement low-impact development techniques. In addition to reducing infrastructure costs, managing stormwater on site can add security through retention facilities that also serve as vehicle barriers and blast setbacks. The design of on-site stormwater infrastructure can

also reduce the need for culverts, drainage pipes, manholes, and other covert site access and weapon concealment opportunities.

In some cases, permit and fee waivers can be used to promote public transportation, which can reduce urban sprawl and traffic congestion, thus helping to decrease the vulnerability of high-risk sites by curbing the flow of traffic and construction of new buildings in high-risk areas. Similarly, creation of an overlay zone (sub-zoning to address area-specific considerations) based on security requirements could firmly establish antiterrorism as a key design consideration, but it could also cause the “branding” of an area as dangerous or high risk, thus jeopardizing the success of any development nearby.

Land use tools for antiterrorism and security are generally derivative in nature and may not be initially obvious. Typically, land use documents contain a wealth of data that can be used to address antiterrorism and security objectives. These sources of information, and many more, are available through a variety of channels, including city, county, and metropolitan planning offices, emergency management offices, tax assessors, councils of governments, and other state and local agencies.

For land use design, designers should consider external and internal aspects. External aspects involve the characteristics of the surrounding area, including construction type, occupancies, and the nature and intensity of adjacent activities, as well as the implications of these characteristics for the protection of the people, property, and operations on the site under consideration. Internal aspects include the amount of land available on the site for stand-off and the inherent ability of the site to accommodate the implementation of natural and manmade antiterrorism and security design features. It is important to recognize that conflicts sometimes arise between security-oriented site design and conventional site design. For example, open circulation and common spaces (which are desirable for conventional design) may be detrimental to certain aspects of security. Designers must balance protection priorities with the requirements of the Americans

with Disabilities Act Accessibility Guidelines (ADAAG), Uniform Federal Accessibility Standards (UFAS), National Fire Protection Codes (NFPC), and other applicable building codes and standards. To resolve these issues, coordination between the disciplines is critical to the design process.

Whether designing new buildings or evaluating existing ones, the designer should evaluate key protection measures to ensure they are appropriate, desirable, and cost-effective in terms of mitigating the risk of potential terrorist attacks. Security measures must be evaluated carefully to understand which measures are truly beneficial and which are not practical.

When making decisions about site antiterrorism and security, designers should consider the following factors:

- Building footprint(s) relative to total land available
- Building location(s) or, if undeveloped, suitable building location(s) relative to the site perimeter and adjacent land uses; distance between the perimeter fence and improved areas off site
- Access via foot, road, rail, water, and air; suitability to support a secure perimeter
- Current and planned infrastructure and its vulnerabilities, including easements, tunnels, pipes, and rights-of-way
- Infrastructure nodes that constitute single-point vulnerabilities
- Adjacent land uses and occupancies that could facilitate attacks or that are potential targets themselves and thus present collateral damage or cascading failure hazards (see Figure 2-1)
- Proximity to fire and police stations, hospitals, shelters, and other critical facilities that could be of use in an attack
- Natural hazards, susceptibility to subsidence or liquefaction, and other environmental considerations

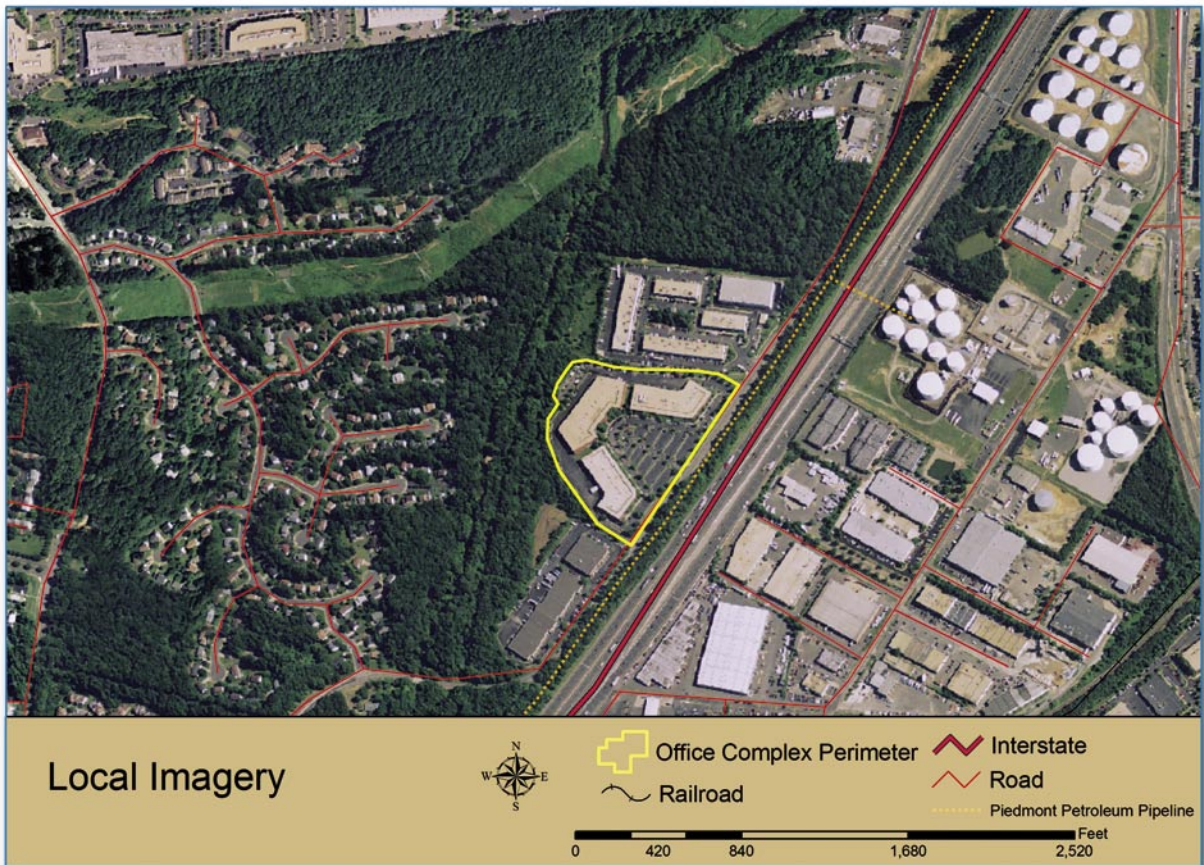


Figure 2-1 An example of using GIS to identify adjacent hazards. Note the large fuel storage and distribution facility (tank farm) in the vicinity of the office building being assessed.

- Presence of natural physical barriers such as water features, dense vegetation, and terrain that could provide access control and/or shielding, or suitability of the site for the incorporation of such features
- Topographic and climatic characteristics that could affect the performance of chemical agents and other weapons
- Observability from outside site boundaries; ability of vegetation in proximity to building or site to screen covert activity

## **2.2 SITE PLANNING**

The single most important goal in planning a site to resist terrorism and security threats is the protection of life, property, and operations. Decision-making in support of this purpose should be based first and foremost on a comprehensive assessment of the manmade threats and hazards so that planning and design countermeasures are appropriate and effective in the reduction of vulnerability and risk. It is important to recognize that a given countermeasure can mitigate one or more vulnerabilities, but may be detrimental to other important design goals. It is also important to think creatively and comprehensively about the security repercussions of common site planning and design decisions. This section will highlight several aspects of site design and will present some of the unique characteristics arising from their application to antiterrorism and security.

### **2.2.1 Site Design**

Because the economics of development dictate recovering the largest possible portion of square footage within most urban and rural sites, security concerns should be evaluated carefully. Conflicts sometimes arise between security site design and conventional site design. For example, open circulation and common spaces, which are desirable for conventional design, are often undesirable for security design. To maximize safety, security, and sustainability, designers should implement a holistic approach to site design that integrates form and function to achieve a balance among the various design elements and objectives. Even if resources are limited, significant value can be added to a project by integrating security considerations into the more traditional design tasks in such a way that they complement, rather than compete with, the other elements.

### **2.2.2 Layout and Form**

The overall layout of a site (e.g., the placement and form of its buildings, infrastructures, and amenities) is the starting point for development. Choices made during this stage of the design process will steer decision-making for the other elements of the site. A



number of aspects of site layout and building type present security considerations and are discussed below.

- **Building placement.** Depending on the site characteristics, the occupancy requirements, and other factors, buildings may be clustered tightly in one area, or dispersed across the site. Both patterns have compelling strengths and weaknesses.

Concentrating people, property, and operations in one place creates a target-rich environment, and the mere proximity of any one building to any other may increase the risk of collateral impacts. Additionally, the potential exists for the establishment of more single-point vulnerabilities in a clustered design than would exist in a more dispersed pattern. However, grouping high-risk activities, concentrations of personnel, and critical functions into a cluster can help maximize stand-off from the perimeter and create a “defensible space.” This also helps to reduce the number of access and surveillance points, and minimize the size of the perimeter needed to protect the facilities. Stand-off planning is discussed in detail in Sections 2.3 and 2.4. In addition, combining multiple uses also provides economic and environmental benefits such as opportunities to efficiently transfer heat from net heat-producing areas and activities to net heat-consuming ones, thus reducing energy costs.

In contrast, the dispersal of buildings, people, and operations across the site reduces the risk that an attack on any one part of the site will impact the other parts. However, this could also have an isolating effect, and reduce the effectiveness of on-site surveillance, increase the complexity of security systems and emergency response, and create a less defensible space.

To the extent that site, economics, and other factors allow, the designer should consolidate buildings that are functionally compatible and have similar threat levels (see Figures 2-2 and 2-3). For example, visitor screening areas, receiving/loading areas, and mailrooms constitute the innermost line of defense,

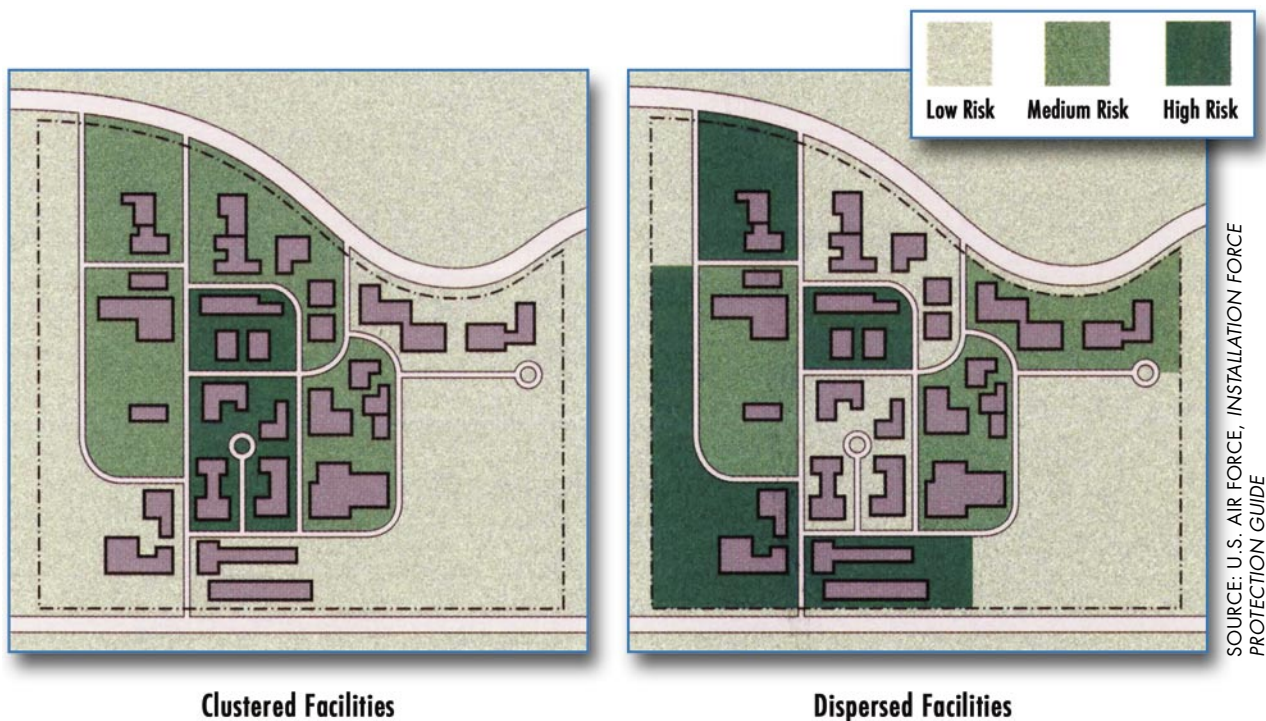


Figure 2-2 Clustered versus dispersed site layouts

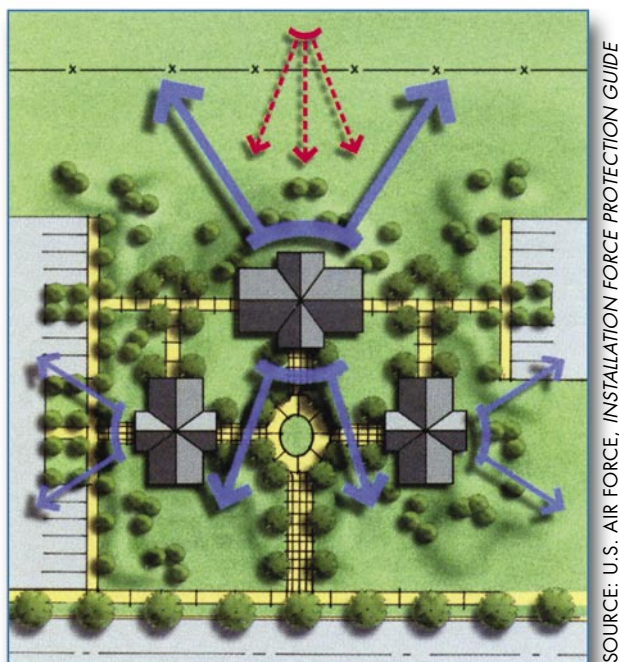


Figure 2-3 Clustering to enhance surveillance opportunities while minimizing views into the buildings

because they may be the first places where people and materials are closely inspected before being introduced into the facility. Logically, they should be physically separated from the key assets such as main operational areas and concentrations of people. It is also desirable to locate potential target buildings away from lower-risk areas in order to minimize collateral damage, should an attack occur.

- **Building orientation.** The orientation of a building can have significant impact on its performance, not only in terms of energy efficiency, but also in the ability to protect occupants. For the purposes of this discussion, the term “orientation” refers to three distinct characteristics: the building’s



spatial relationship to the site, its orientation relative to the sun, and its vertical or horizontal aspect relative to the ground.

A structure's orientation relative to its surroundings defines its relationship to that area. In aesthetic terms, a building can "open up" to the area or turn its back; it can be inviting to those outside, or it can "hunker down" defensively. The physical positioning of a building relative to its surroundings may seem subtle, but can be a greater determinant of this intangible quality than exterior aesthetics. Nevertheless, the proximity of a vulnerable façade to a parking area, street, adjacent site, or other area that is accessible to vehicles and/or difficult to observe can greatly contribute to its vulnerability. This illustrates one way in which protective requirements can be at odds with otherwise good design. A strong, blank wall with no glazing will help to protect the people, property, and operations within from a blast, but the lack of windows removes virtually all opportunity to monitor activities outside and take appropriate protective actions in a timely manner. Designers should consider such trade-offs early in the design process, in an effort to determine an acceptable level of risk.

The solar orientation of a building is a significant factor in energy consumption. By optimizing the positioning of the building relative to the sun, climate control and lighting requirements can be met while reducing power consumption. However, these energy conservation techniques present some important security considerations. For example, natural ventilation is an effective and time-tested technique for efficiently cooling buildings; however, the use of unfiltered outside air presents a major vulnerability to aerosolized chemical, biological, and radiological agents, in addition to accidental releases of hazardous materials. Additionally, awnings may become projectiles in a blast event, and the construction of operable windows may not be as blast-resistant as the frames of fixed windows. Similarly, the use of light shelves, skylights, clerestories, and atria can help meet illumination requirements while dramatically reducing

the need for electric lighting. However, day lighting relies inherently on the use of glazing, which has been shown to be one of the major hazards in blast events. In addition to ensuring the maximum setback possible for highly-fenestrated facades, designers should ensure that aperture sizes, glazing materials, films, and frames and connections are selected with blast-resistance as well as energy efficiency in mind.

- **Open space.** The incorporation of open space into site design presents a number of benefits. First and foremost is the ability to easily monitor an area and detect intruders, vehicles, and weapons. Closely related to this benefit is the stand-off value of open space; as discussed in Chapter 4, blast energy decreases as the inverse of the cube of the distance from the seat of the explosion, so every additional increment of distance provides increasingly more protection. In addition, pervious open space allows stormwater to percolate back into the ground, reducing the need for culverts, drainage pipes, manholes, and other covert site access and weapon concealment opportunities. Also, if the open space is impassible for vehicles (as in the case of a wetland or densely vegetated area), it can provide not only environmental and aesthetic amenities, but prevent vehicle intrusion as well.

Leaving significant amounts of open space, wetland, or other sensitive areas unimproved may present opportunities to reap economic benefits in the form of transferable development rights (TDRs). TDR is a market-based approach that provides incentives to developers to focus growth only where it is desired, making it profitable to refrain from developing open space and sensitive areas. By not maximizing the profit potential of their land, owners can receive “development right credits” that can be sold to developers elsewhere in the community, who will then be able to use those credits to intensify the use of their own land in ways that promote more sustainable growth.<sup>1</sup> Thus, in some cases, TDRs may be a windfall benefit of security-oriented development.

<sup>1</sup>U.S. EPA, *Smart Growth Policy Database*. <http://cfpub.epa.gov/sgpdb/sgdb.cfm>

### 2.2.3 Vehicular and Pedestrian Circulation

The movement of people and materials into, through, and out of a facility is determined by the design of its access, circulation, and parking systems. Such systems should be designed to maximize efficiency while minimizing conflicts between vehicle and pedestrian modes. Designers should begin with an understanding of the site's transportation requirements based on an analysis of how the facility will be used. This includes studying the number and types of access points that are required, the parking volume needed, pedestrian patterns, and the modes of transportation they will use. Several aspects of transportation planning can impact security and are discussed below.

- **Roadway network design.** Streets are generally designed to minimize travel time and maximize safety, with the end result typically being a straight path between two or more endpoints. Although a straight line may be the most efficient course, designers should use caution when orienting streets relative to buildings. Given that the energy transferred when one object strikes another is a function of its mass and its velocity, a bollard that can stop a 15,000-pound truck moving at 35 miles per hour may not be able to stop the same truck moving at 55 miles per hour. In developing a system of street alignments with protection in mind, the designer cannot determine the size or weight of a vehicle that will travel along the road, because that is a management decision. However, the designer can propose a roadway system to minimize vehicle velocity, thus using the roadway itself as a protective measure. This is accomplished through the use of the following strategies.

First, straight-line or perpendicular approaches to buildings should not be used, because these give vehicles the opportunity to gather the speed necessary to ram through protective barriers and crash into or penetrate buildings. Instead, approaches should be parallel to the façade, with berms, high curbs, appropriate trees, or other measures used to prevent vehicles from departing the roadway. A related technique for reducing vehicle speeds is the construction

of serpentine (curving) roadways with tight-radius corners. Existing streets can be retrofitted with barriers, bollards, swing gates, or other measures to force vehicles to travel in a serpentine path. Again, high curbs and other measures should be installed to keep vehicles from departing the roadway in an effort to avoid these countermeasures.

Less radical than these techniques are traffic calming strategies, which seek to use design measures to cue drivers as to the acceptable speed for an area. These include raised crosswalks, speed humps and speed tables, pavement treatments, bulbouts, and traffic circles. In addition to creating a more pedestrian-friendly environment, which increases “eyes on the street” surveillance, designing roadways to physically limit speeds can have the added benefits of increasing safety and, subsequently, lowering liability. Designers should be aware, however, that many of these techniques can have detrimental effects for emergency response, including slowing response time, interfering with enroute emergency medical treatment, and increasing the difficulty of maneuvering fire apparatus. They also may present problems for snow removal, and their outer ends should remain flat so that bicycles can proceed unimpeded. Finally, the distinction between speed humps, speed tables, and speed bumps is critical. Speed humps and tables are much gentler than speed bumps and can be constructed to “enforce” a specific speed range. Speed bumps have much more abrupt profiles and are only appropriate for low-speed applications, such as parking lots.

- **Parking.** There are three primary types of parking facilities, all of which present security trade-offs. Surface lots can be designed to keep vehicles away from buildings, but they consume large amounts of land and, if constructed of impervious materials, can contribute greatly to stormwater runoff volume. They can also be hazardous for pedestrians if dedicated pedestrian pathways are not provided. In contrast, on-street parking is often convenient for users and a source

of revenue for local governments, but this type of parking may provide little or no setback. Finally, garage structures provide revenue and can be convenient for users, but they may require structural measures to ensure blast resistance as well as crime prevention measures to prevent street crime. Although the cost of land suggests that the construction of a garage below a building (either underground or aboveground) may be the most economically viable approach for many developments, they can be highly vulnerable to vehicle-borne weapons, endangering the building above. If garages must be used, human security procedures (e.g., vehicle searches) and electronic systems (e.g., closed circuit television) may be necessary to ensure safety (see Section 2.7 for additional information).

#### **2.2.4 Infrastructures and Lifelines**

Providing power, gas, water, wastewater, and communications services is one of the most basic requirements of any development. At the site scale, all critical lifelines should have at least one layer of redundancy, or backup. By eliminating single-point vulnerabilities, designers reduce the chance that service will be interrupted if an attack damages or destroys a lifeline either outside the perimeter or on site. It is important to note that collocating a backup lifeline with its primary lifeline does not eliminate single-point vulnerability; only physical separation can substantially increase the likelihood of continuity of service. Designers should be aware that this could create the need for each type of infrastructure lifeline to cross the site perimeter at multiple locations, potentially complicating the process of managing utility easements and rights-of-way. Additional information on critical systems is also discussed in Chapter 3.

Additionally, all controls, interconnections, exposed lines, and other vulnerable elements of infrastructure systems should be protected from access and exploitation by surveillance and/or physical countermeasures. Service entrances and other secondary access points should be monitored and access-controlled; special

attention should also be paid to any locations where multiple systems or primary and backup systems come together, such as control rooms and mechanical spaces. Again, these facilities should be designed for maximum observability, including the use of opportunity reduction and target hardening strategies where appropriate, and should be equipped with adequate lighting and emergency communications capabilities wherever possible.

### **2.2.5 Landscape and Urban Design**

Designing to meet user needs while maintaining stewardship of the natural and built environments becomes increasingly more challenging when security requirements are factored in. Design principles should include an emphasis on mixed-use development; selection of low-impact development techniques and environmental stewardship; compatibility of context and relationship with adjacent uses, forms, and styles; establishment of scale and identity through aesthetic design; connectivity among buildings, uses, activities, and transportation modes; resource conservation; cultural responsiveness; and the creation of appealing public spaces. These objectives are generally achieved through the work of two closely related disciplines, landscape design and urban design. For the purposes of this document, these two domains are virtually overlapping and will, therefore, be addressed together.

- **Landscape design.** The implications of security for landscape design affect everything from plant species and building material selection to landform construction and wayfinding. Elements such as landforms, water features, and vegetation are among the building blocks of attractive and welcoming spaces, and they can also be powerful tools for enhancing security. These features can be used not only to define or designate a space, but also to deter or prevent hostile surveillance and unauthorized access. Vegetative groupings and landforms can even provide some level of blast shielding. Stands of trees, earthen berms, and similar countermeasures generally cannot replace setbacks, but they can offer supplementary protection. However, landscaping

can also have detrimental impacts for safety and security, and practitioners should consider the unique requirements of the project to ensure that the landscape design elements they choose will be appropriate and effective.

For example, thorn-bearing and sharp-leaved plant species (e.g., firethorn, Spanish bayonet, and pampas grass) can create natural physical barriers to deter aggressors. Although this technique can be highly effective, designers should consider the liability they may incur from injuries resulting from legitimate users inadvertently coming into contact with them. Additionally, although such plants can provide security for ground-level windows, they may also impede emergency egress.

With careful selection, placement, and maintenance, landscape elements can provide visual screening that protects sensitive operations, gathering areas, and other activities from surveillance without creating concealment for covert activity. However, dense vegetation in close proximity to a building can screen illicit activity and should be avoided. Additionally, thick ground cover such as English ivy or vegetation over 4 inches tall such as monkey grass can be used to conceal bombs and other weapons; in setback clear zones, vegetation should be selected and maintained with eliminating concealment opportunities in mind. Similarly, measures to screen visually detractive components such as transformers, trash compactors, and condensing units should be designed to minimize concealment opportunities for people and weapons.

- **Urban design.** Through urban design, practitioners seek to create vibrant, inviting, and functional places for people to live, work, and play. To protect people, property, and operations, and to reduce liability, security should be considered a necessary aspect of these characteristics. If people do not feel safe, they will not use a place and, if a place is not used as intended, it will fail to fulfill its purpose. This failure can, in turn, result in a net loss to the community in terms of social, economic, and environmental sustainability.

Numerous urban design elements present opportunities to provide security. The scale of the streetscape should be appropriate to its primary users, and it can be manipulated to increase the comfort level of desired users while creating a less inviting atmosphere for users with malicious intent. However, even at the pedestrian scale, certain operational requirements must be accommodated. For example, although efficient pedestrian and vehicle circulation systems are important for day-to-day living, they are also critical for emergency response, evacuation, and egress. Furthermore, despite an emphasis on downsizing the scale of the streetscape, it is critical to maintain the maximum stand-off distance possible between vehicles and structures.

At the site perimeter, walls and fences used for space definition may be hardened to resist the impact of a weapon-laden truck; however, planters, bollards, or decorative boulders could accomplish the same objective in a much more aesthetically pleasing manner. Such an approach also creates permeability, which would allow pedestrians and cyclists to move more easily through the space. Additional information on protective barriers is included in Section 2.4.1.

Similarly, street furniture (e.g., mailboxes, bus stop shelters, light poles, works of art, street trees, planters, bicycle racks, seating, newspaper boxes, kiosks, and trash receptacles) can be used to enhance security (see Figure 2-4). For example, bus stop shelters can be designed to allow for easy surveillance and detection of suspicious activity and objects. Hardened versions of everyday items, such as light poles, planters, benches, street trees (of appropriate size and type), and even water fountains can serve as vehicle barriers. These items maintain stand-off while creating a line of protection that is virtually transparent and highly permeable at the pedestrian scale. Note that in-ground installation of bollards, fences, and any other anti-ram measures should be preceded by an assessment of soil conditions and underground utilities in the immediate vicinity.



SOURCE: NATIONAL CAPITAL URBAN DESIGN AND SECURITY PLAN, NATIONAL CAPITAL PLANNING COMMISSION, 2002

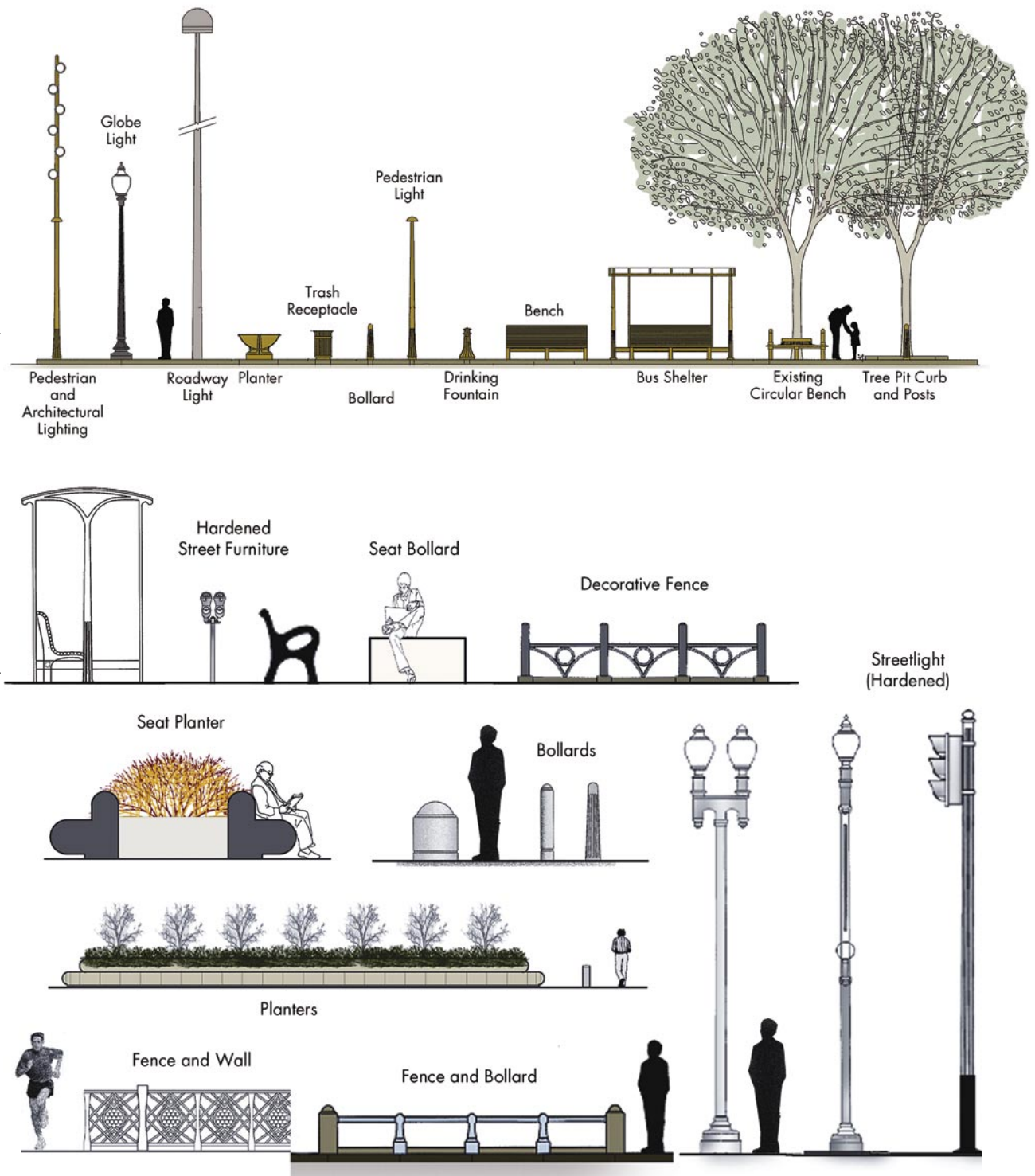


Figure 2-4 Streetscape security elements

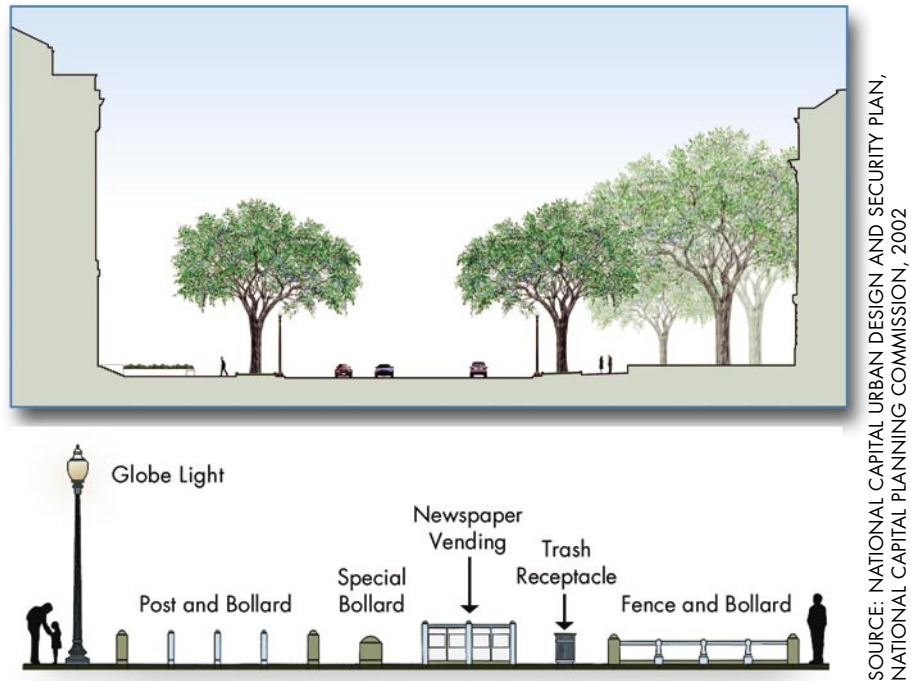


Figure 2-4 Streetscape security elements (continued)

A main challenge for the design community is to reach the desired level of protection without turning the building or facility into a bunker or fortress. In other words, they are required to incorporate subtle and aesthetically pleasing security measures when involved in urban design projects. Below are some rules of thumb that should be taken into consideration when designing an urban landscape with a security component:

- Security measures must not impede access to public entrances or pedestrian flow on adjacent sidewalks.
- Landscape elements in the form of grassed plinths, trees, plantings, fountains, and pools are appropriate, but must be designed as integral parts of a building and its setting as much as possible.
- Miscellaneous decorative elements such as flag poles, fountains, pools, gardens, and similar features may be located within an accessway to slow movement or restrict access.

- Trees planted along the inside edge of a public sidewalk and adjacent to pedestrian and vehicular accessways can serve dual aesthetic and barrier purposes.
- The design of bollards, fences, light posts, and other streetscape and landscape elements should form an urban ensemble that helps to create a sense of unity and character.
- Security devices must be designed and located to establish consistent, rhythmic patterns along the street, particularly where a number of elements are used in combination to reduce visual street clutter.
- Security devices must not obstruct pedestrian movement or access by emergency vehicles; therefore, the use of bollards, posts, and chains may be inappropriate when this function is required.

No discussion of using landscape and urban design for security would be complete without a discussion of design-oriented crime prevention strategies such as Crime Prevention Through Environmental Design (CPTED). This approach to design is based on evidence that the design and form of the built environment can influence human behavior. Specifically, CPTED seeks to create a physical environment that discourages criminal activity by incorporating territoriality cues, natural access controls, natural surveillance, support for legitimate activities, and ongoing property maintenance into landscape and urban design. Section 2.12 is a brief overview of CPTED.

Closely related to, but not synonymous with, CPTED is situational crime prevention. This approach encompasses many CPTED principles; however, it focuses on managerial and user behavior factors that affect opportunities for criminal behavior in a specific setting for a specific crime, whereas CPTED focuses on changing the physical design aspects of environments to deter criminal activity. More akin to CPTED is the defensible space approach, in which the emphasis is on structuring the physical layout of space so that its residents are able to establish a sense of ownership and control over common areas in the community. Both of these proactive approaches to crime prevention have merit; designers should care-

fully evaluate the unique requirements of each design problem to identify the most appropriate strategy.

Landscape and urban design inherently define the “line of sight” in a space. Operational security is not a traditional element of master planning, but managing the threat of hostile surveillance is a significant consideration in protecting people, property, and operations. These techniques seek to deny aggressors a “line of sight” to a potential target, either from on or off site. This increases the protection of sensitive information and operations by using stand-off weapons (see Figures 2-5 and 2-6). In addition to the use of various screening options, anti-surveillance measures (e.g., building orientation, landscaping, screening, and landforms) can also be used to block sight lines.

Depending on the circumstances, landforms can be either beneficial or detrimental to anti-surveillance. Elevated sites may enhance surveillance of the surrounding area from inside the facility, but may also allow observation of on-site areas by adversaries. Buildings should not be sited immediately adjacent to higher surrounding terrain, unsecured buildings owned by unfamiliar parties, or vegetation, drainage channels, ditches, ridges, or culverts that can provide concealment. For high-risk buildings, it may be necessary to provide additional protection by creating a clear zone immediately adjacent to the structure that is free of all visual obstructions or landscaping (see Figure 2-7). The clear zone fa-

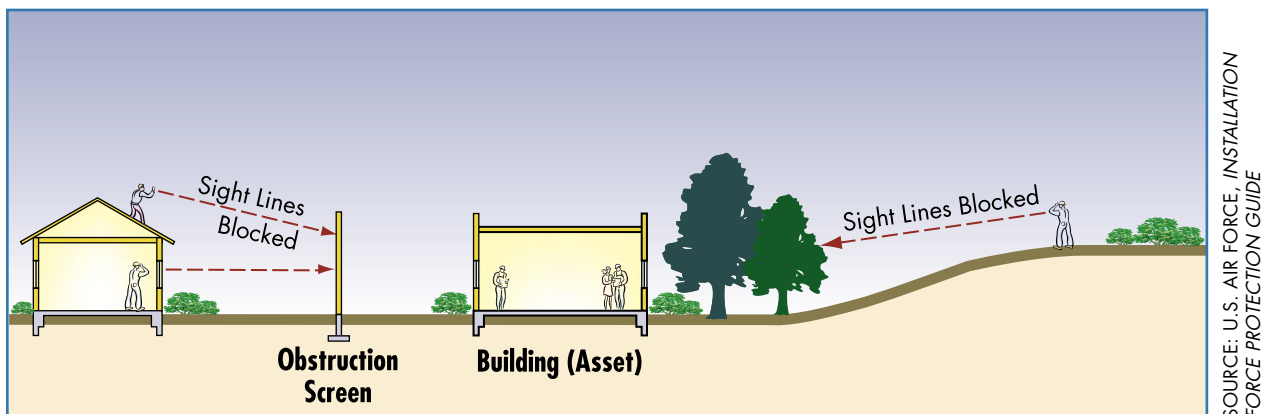


Figure 2-5 Blocking of sight lines

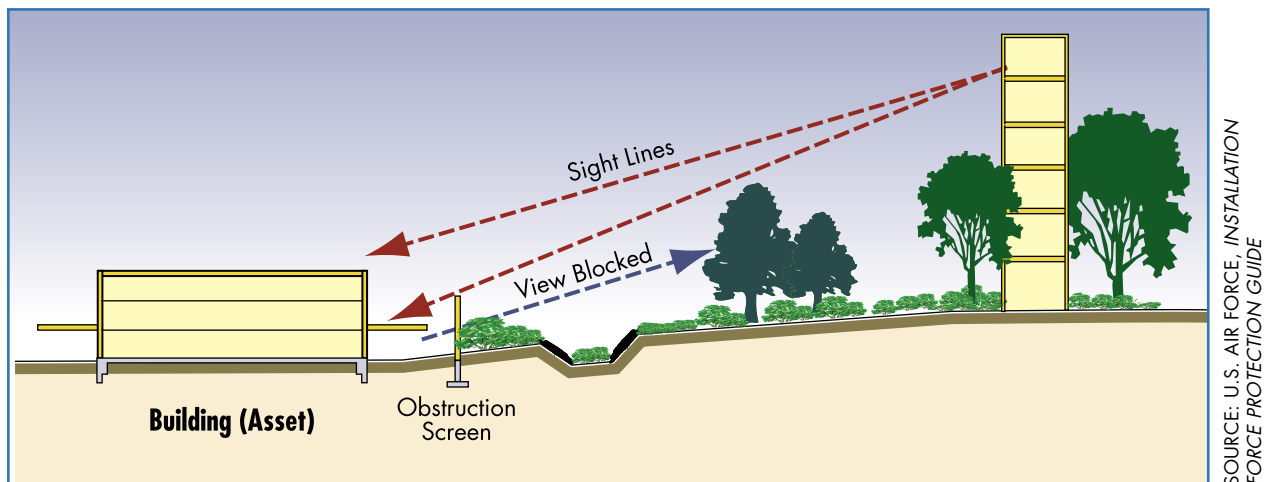


Figure 2-6 Improper building siting and view relationships

Facilitates monitoring of the immediate vicinity and visual detection of attacks. Walkways and other circulation features within a clear zone should be located so that buildings do not block views of pedestrians and vehicles. If clear zones are implemented, it may be necessary to implement other anti-surveillance measures.

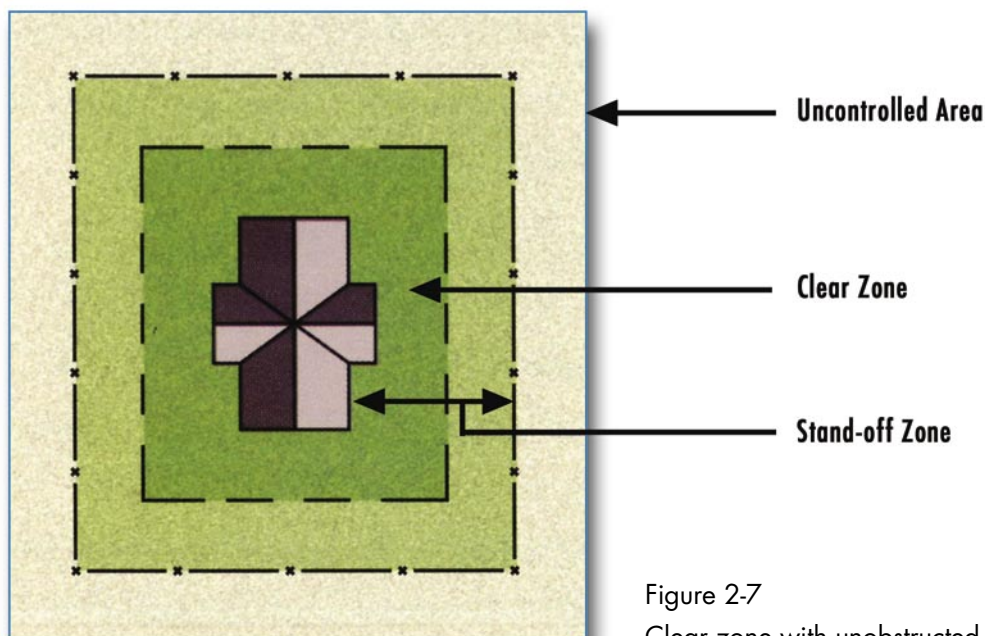


Figure 2-7  
Clear zone with unobstructed views

SOURCE: U.S. AIR FORCE, INSTALLATION FORCE PROTECTION GUIDE



## 2.3 STAND-OFF DISTANCE

Many different measures can be used to provide site design protection. Distance is the most effective and desirable tool because other measures vary in effectiveness, are more costly, and often have unintended consequences. For example, a blast wall can become the source of fragmentation if an explosion occurs in close proximity to it. The most cost-effective solution for mitigating explosive effects is to ensure the explosions occur as far away from the buildings as possible. Stand-off distance and the effects of blast are discussed in Section 4.2.

The distance between an asset and a threat is referred to as the stand-off distance, as shown in Figure 2-8. There is no ideal stand-off distance; it is determined by the type of threat, the type of construction, and desired level of protection. The primary design strategy is to keep terrorists away from inhabited buildings (see Figure 2-9). Although sufficient stand-off distance is not always possible in conventional construction, maximizing the distance may be the most cost-effective solution. Maximizing stand-off distance also ensures that there is opportunity in the future to upgrade buildings to meet increased threats or to accommodate higher levels of protection. Stand-off distance must be coupled

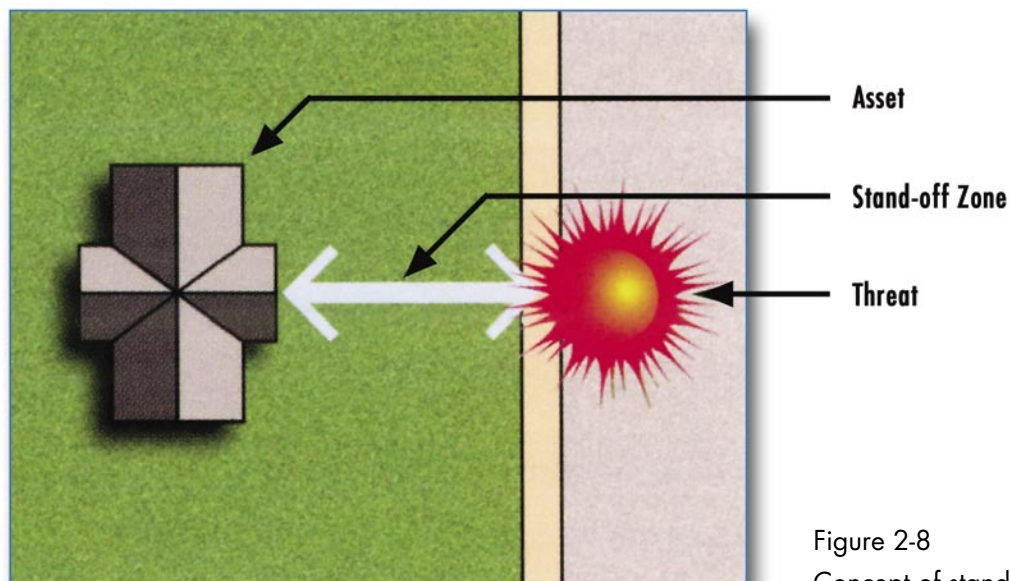


Figure 2-8  
Concept of stand-off distance

SOURCE: U.S. AIR FORCE, *INSTALLATION FORCE PROTECTION GUIDE*

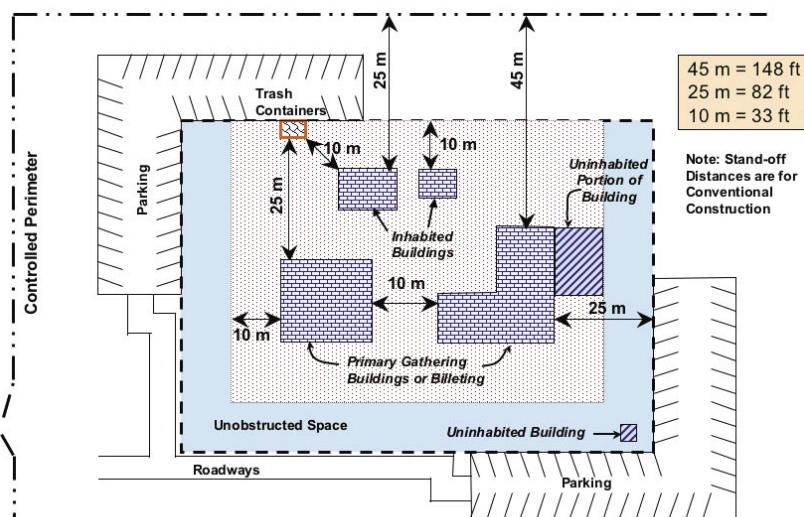
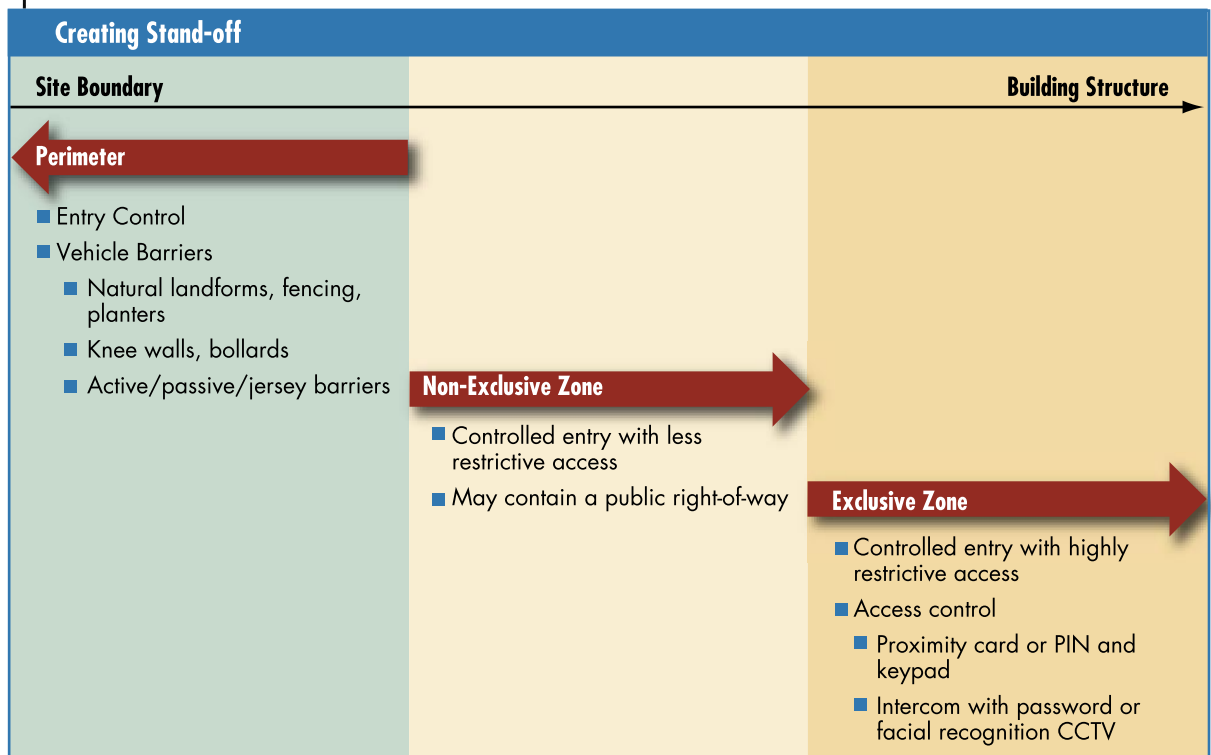


Figure 2-9  
Stand-off distance and  
building separation



with appropriate building hardening, as discussed in Chapters 3 and 4, to provide the necessary level of protection to assets. Considerations for stand-off distance are as follows:

- The first mode of site protection is to create “keep out zones” that can ensure a minimum guaranteed distance between an explosion (e.g., from a vehicle) and the target structure.

- The perimeter line is the outermost line that can be protected by the security measures incorporated during the design process. It is recommended that the perimeter line be located as far as is practical from the building exterior. Many vulnerable buildings are located in urban areas where only the exterior wall of the building stands between the outside world and the building occupants. In this case, the options are obviously limited. Often, the perimeter line can be pushed out to the edge of the sidewalk by means of bollards, planters, and other obstacles, as discussed earlier in this chapter. To push this line even further outward, restricting or eliminating parking along the curb often can be coordinated with local authorities. In some extreme cases, elimination of loading zones and the closure of streets are an option.
- “Keep out zones” can be achieved with perimeter barriers that cannot be compromised by vehicular ramming. A continuous line of security should be installed along the perimeter of the site to protect it from unscreened vehicles and to keep all vehicles as far away from critical assets as possible.
- When selecting a site for a building, consider its location relative to the site perimeter. Maximize the distance between the perimeter fence and developed areas, providing as much open space as possible inside the fence along the site perimeter.
- The following critical building components should be located away from main entrances, vehicle circulation, parking, and maintenance areas. If this is not possible, harden as appropriate:
  - Emergency generator, including fuel systems, day tank, fire sprinkler, and water supply
  - Normal fuel storage
  - Telephone distribution and main switchgear
  - Fire pumps
  - Building control centers
  - UPS systems powering critical functions



- Main refrigeration systems if critical to building operation
- Elevator machinery and controls
- Shafts for stairs, elevators, and utilities
- Critical distribution feeders for emergency power

## **2.4 CONTROLLED ACCESS ZONES**

One method to attain the appropriate level of protection and ensure stand-off distance between assets and potential threats is with the creation of a controlled access zone. These zones attempt to limit access to the area immediately surrounding a building. Access to a controlled zone can be restricted by the installation of a physical barrier. Although a controlled access zone is one of the best methods of providing stand-off, such issues as site limitations, building siting, and property line restrictions do not always allow this zone to be created. For additional references, see building placement information in Section 2.2.2.

For high-risk building sites, there is a broad range of “controlled access” elements in security design. Controlled access may range from a complete physical perimeter barrier (full control), to relatively minimal anti-vehicle protection with full pedestrian access, to simply monitoring the perimeter with electronic means.

A good way to ensure appropriate stand-off distance is by establishing controlled zones. These zones define minimum distances between assets and potential threats through the installation of barriers (such as bollards, planters, fountains, walls, and fences), as explained in Section 2.2.5. The barriers are designed to withstand assaults by terrorist vehicles; however, their placement must be designed to allow for access by fire and rescue vehicles in the event of an emergency. Selection of barriers is based on operational considerations related to vehicle access and parking. Good design principles for high-risk buildings endorse the complete surround of a building with a stand-off zone that has perimeters set at distances that consider threat levels, desired level of protection,

building construction, and land availability. Entry into a controlled area should only be through an entry control point.

Controlled access zones may be exclusive or non-exclusive, as shown in Figure 2-10. An exclusive zone is the area surrounding a building within the exclusive control of the building. Anyone entering an exclusive zone must have a purpose related to the building. A non-exclusive zone is either a public right-of-way or an area related to several buildings. Someone entering a non-exclusive zone could be headed for any building within that area. Public access areas outside a downtown building would typically be considered non-exclusive. As explained previously, these measures may not be applicable for all buildings. They are intended for those who need security measures due to their function or location.

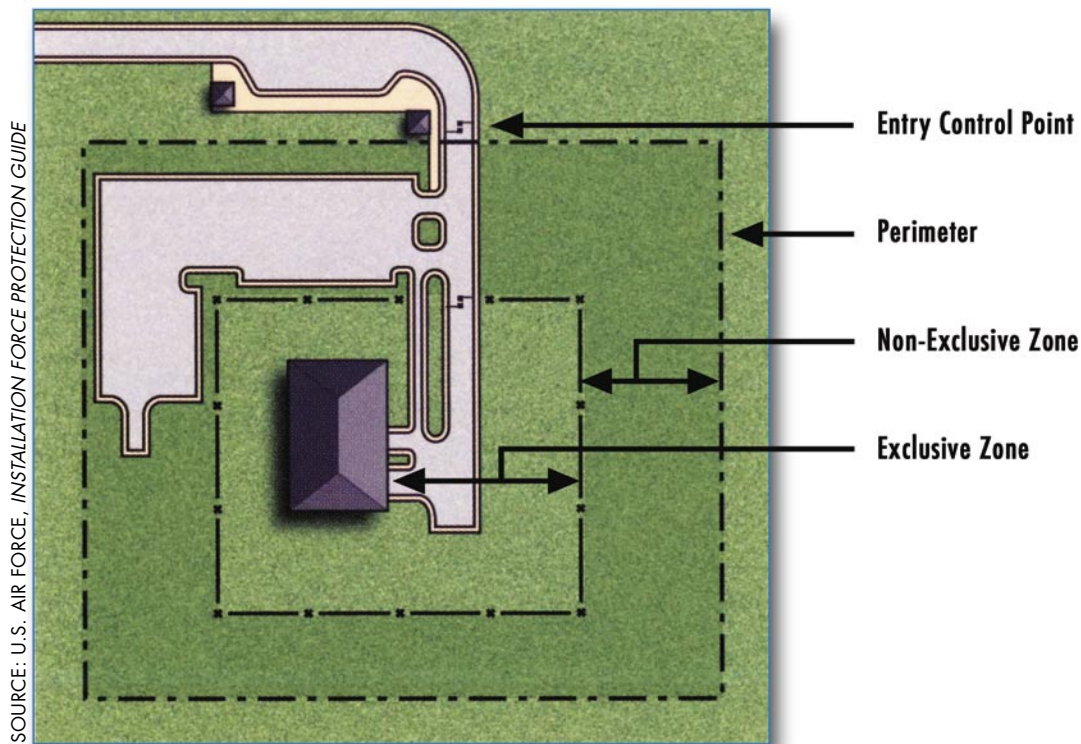


Figure 2-10 Exclusive and non-exclusive zones

### **2.4.1 Physical Protective Barriers**

A physical barrier is a means of establishing a controlled access area around a building or asset. Physical barriers can be used to define the physical limits of a building or campus and can help to restrict, channel, or impede access and constitute a continuous obstacle around the site. Physical barriers can create a psychological deterrent for anyone planning an unauthorized entry and they can delay or prevent passage into a site. This is especially true of barriers against forced entry by vehicles. The type of barriers utilized can have a direct impact on the number and type of security posts that may be needed to ensure site security. Utility areas (such as water sources, transformer banks, commercial power and fuel connections, heating and power plants, or air conditioning units) may require these barriers for safety standards.

As explained in Section 2.2.5, a number of elements may be used to create a physical barrier, some natural and some manmade. Natural barrier elements include rivers, lakes, waterways, steep terrain, mountains, barren areas, plants, and other terrain features that are difficult to traverse. Manmade elements include fencing, walls, buildings, bollards, planters, concrete barriers, and fountains. Selection of elements must consider the level of security desired and the type of threat most likely to occur. Some perimeter security elements are shown in Figure 2-11.

Fencing is a common means of establishing a physical protective barrier to protect a controlled area. The type of fencing used depends primarily on the threat and the degree of permanence. It may also depend on the availability of materials and the time needed for construction. Fencing may be erected for other uses besides impeding personnel access, such as obstructing views, serving as a means to defeat stand-off weapon systems (e.g., rocket-propelled grenades), and serving as a barrier to hand-thrown weapons (e.g., grenades and firebombs).

Fencing may be used to augment or increase the security of existing barriers that protect restricted areas. Examples include the creation an additional barrier line and an increase in the existing

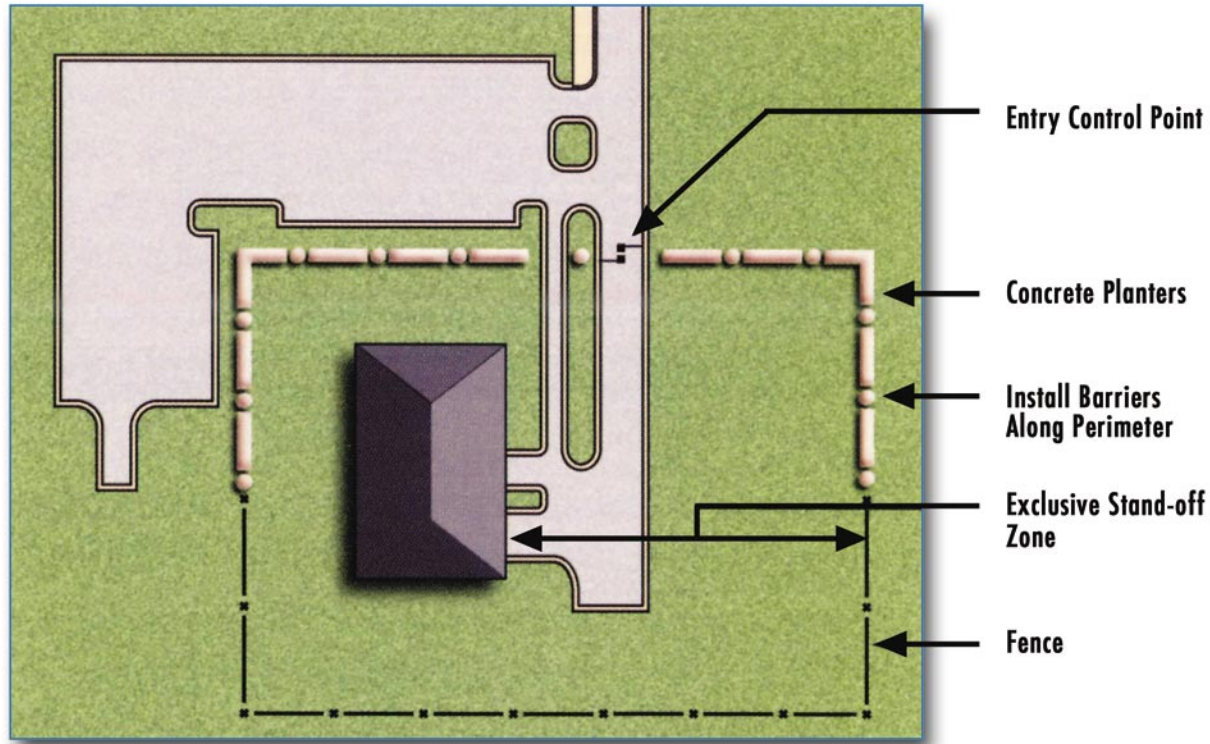


Figure 2-11 Application of perimeter barrier elements

fence height. It is important to recognize that fencing provides very little delay when it comes to motivated aggressors, but it can act as a psychological deterrent when an aggressor is deciding which building to attack. The following are commonly used fencing types:

- **Chain-link.** Generally, chain-link fencing is used for protecting permanent limited and exclusion areas. Chain-link fence (including gates) is typically 6-foot high fence fabric, mounted on steel poles that may include a top guard or outrigger. Chain-link fences are usually 9-gauge or heavier, galvanized wire with mesh openings not larger than 2 inches per side and have twisted and barbed selvages at the top and the bottom.
- **Anti-climb (CPTED) fence.** Although different styles of anti-climb fences are available, most consist of vertical bars with horizontal supports designed to make climbing difficult.

- **Barbed wire.** Standard barbed wire is twisted, double-strand wire, with four-point barbs spaced an equal distance apart along the strand. Barbed wire fencing (including gates) intended to prevent human trespassing should not be less than 6 feet high and must be affixed firmly to posts not more than 6 feet apart. Barbed wire may be used as a top guard or outrigger on a standard chain-link fence.
- **Barbed tape or concertina.** A barbed taped obstacle fabricated from 0.025-inch stainless steel tape with barbed clusters. Barbed tape can be deployed, tangle-free, for fast installation without supporting fence posts.
- **Triple-standard concertina wire.** This type of fence uses three rolls of stacked concertina; one roll is stacked on top of two other rolls that run parallel to each other while resting on the ground, forming a pyramid. This fence has been used effectively in lieu of a chain-link fence.
- **Tangle-foot wire.** Tangle-foot wire is an obstruction fence constructed of barbed wire or tape set up outside a single perimeter fence or in the area between double fences to provide an additional deterrent to intruders. Wire or tape is supported on short metal or wooden pickets spaced at irregular intervals of 3 to 10 feet and at heights between 6 and 12 inches. The wire or tape should be criss-crossed to provide a more effective obstacle. The space and materials available govern the depth of the field. Liability issues should be considered when installing a tangle-foot wire.
- **Cable.** Cable or wire rope can be used as a separate, temporary barrier or it may be attached to chain-link or anti-climb fences to provide additional crash resistance.

When necessary, a top guard should be installed on all perimeter fences and may be added to interior enclosures for additional protection. A top guard is an overhang of barbed wire or tape along the top of a fence, facing outward and upward at approximately a 45-degree angle. Placing barbed wire or tape above it can further enhance the top guard. Top guard supporting arms are perma-

nently affixed to the top of fence posts and increase the overall height of the fence. Three strands of barbed wire spaced 6 inches apart must be installed on the supporting arms. (Due to liability issues in some locations, the top guards will not be allowed to face outward where the fence is adjacent to public areas.)

Clear zones should be maintained on both sides of the perimeter barrier to provide an unobstructed view of the barrier and the ground adjacent to it. A clear zone of 20 feet or more should exist between the perimeter barrier and exterior structures, parking areas, and natural or manmade features. When possible, a clear zone of 50 feet or more should exist between the perimeter barrier and structures within the protected area, except when the wall of a building constitutes part of the perimeter barrier. Roads within the clear zone should be as close to the perimeter barrier as possible without interfering with it. The roads should be constructed to allow effective road barriers to deter motor movement of unauthorized personnel. When barriers enclose a large area, a perimeter road should be provided for security patrol vehicles on the interior.

Fences may be augmented with additional security systems, such as motion sensors and closed circuit camera systems.

Because barriers can be compromised through breaching (cutting a hole through a fence) or by nature (berms eroded by the wind and rain), they should be inspected and maintained at least weekly. Security personnel should look for signs of deliberate breaches, holes in and under barriers, natural debris building up against barriers, and the proper functioning of locks.

### **2.4.2 Other Perimeter Barriers**

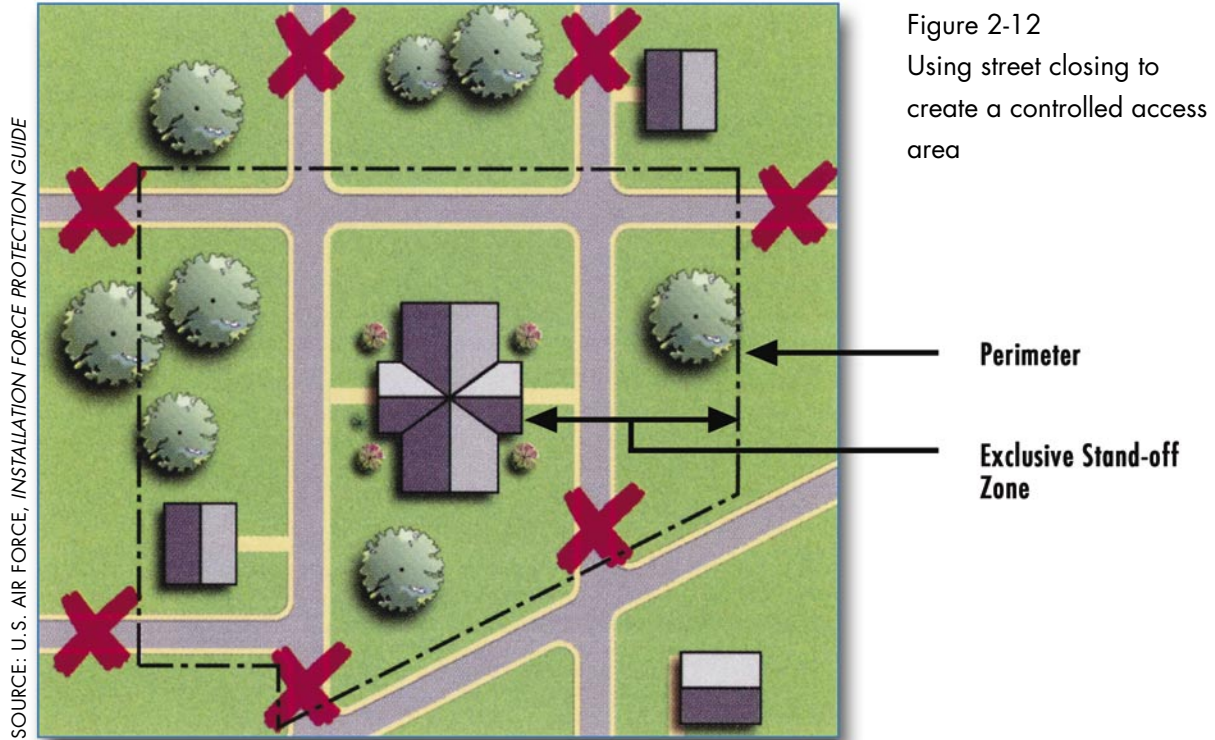
The exterior of a building may form a part of a perimeter barrier. Brick or block masonry or cast in place concrete walls may act as part of a perimeter barrier. They must be at least 7 feet high and should have a barbed wire top guard, depending on the threat and application. The windows, active doors, and other designated openings should be pro-



tected with fastening bars, grilles, or chain-link screens, and window barriers should be fastened from the inside. If hinged, the hinges and locks must be on the inside to facilitate emergency egress.

Barrier walls designed to resist the effects of an explosion can, in some cases, act to reduce the pressure levels acting on the exterior walls of buildings. They may not, however, enhance security because they prohibit observation of activities occurring on the other side of the wall. In this case, a plinth wall (anti-ram knee wall) with a fence may be an effective solution to combine anti-ram capability and observation.

Consideration should also be given to the improvement of a defensive posture should threat levels increase. A number of temporary or semi-permanent measures may be effective. Expedient methods include blocking access routes with heavy vehicles or temporarily blocking roads surrounding a building to create a form of controlled access area. Figure 2-12 is an example of closing streets to restrict access around a building.



Typically, street closures exclude vehicles, but allow access by pedestrians with proper credentials. The use of street closures must be balanced against minimum circulation/access requirements and fire protection considerations.

If a secured area requires a limited exclusion area on a temporary or infrequent basis, it may not be possible to use physical structural barriers. A limited exclusion area may be established with additional security posts, patrols, and other security measures during the period of restriction. Temporary barriers (including temporary fences, jersey barriers, and vehicles) may also be used.

### **2.4.3 Anti-ram Vehicle Barriers**

Vehicle barriers are a traditional anti-ram solution that prevents vehicle access for pedestrian protection and building security. Vehicle barriers are considered either passive barriers, which are stationary (e.g., fixed bollards, concrete walls, planters, berms), or active barriers, which can typically be retracted or moved out of the way to allow passage (such as retractable bollards, crash beams, and rotating plates). Passive barriers are used to create perimeter or edge protection; active barriers are applicable to roadways, driveways, or entry control points where they can be lowered or raised to prevent passage.

Passive barriers typically consist of bollards, which are concrete filled steel pipes that can be placed every few feet along the curb of a sidewalk to prevent vehicle intrusion (see Figure 2-13). In order to resist the impact of a vehicle, the bollard needs to be fully embedded into a concrete strip foundation that is several feet deep. The height of the bollard above ground should be higher than the bumper of the vehicle, typically 39 to 40 inches. The spacing of the bollards is based on several factors, including Americans with Disabilities Act (ADA) requirements, the minimum width of a vehicle, and the number of bollards required to withstand the impact. As a rule of thumb, the center to center spacing should be between 3 and 5 feet to be effective. The foundation should be designed according to site soil conditions.



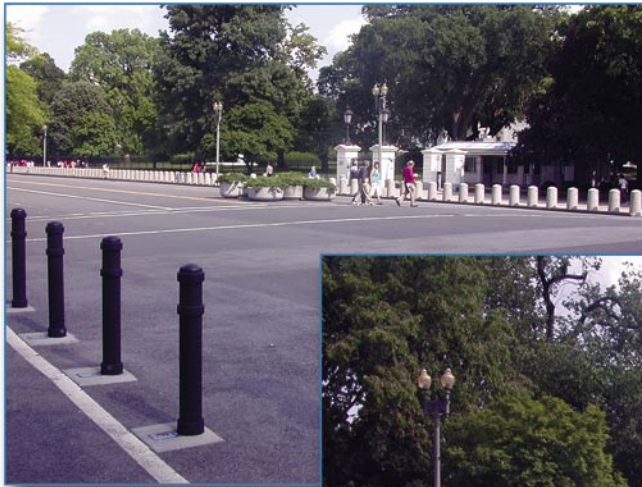


Figure 2-13  
Sample bollard applications



An alternative to a bollard is a plinth wall, which is a continuous low wall constructed of reinforced concrete with a buried foundation. The bollard or plinth wall is designed by equating the kinetic energy of the vehicle at impact with the strain energy absorbed by the barrier and the vehicle.

The foundation of the bollard and plinth wall system can present challenges. For effectiveness, the barriers need to be placed as close to the curb as possible. The property line of buildings often does not extend to the curb. Therefore, a permit may be required by the local authorities to place barriers with foundations near the

curb. To avoid this, building owners are often inclined to place bollards along the property line, which significantly reduces the effectiveness of the barrier system because it reduces the stand-off distance. Sometimes a basement may exist below the pavement that extends to the property line. Embedding a barrier foundation into the basement foundation wall or through the basement roof may introduce water infiltration issues and structural foundation design complications.

Another problem that can arise is below ground utilities that may be close to the pavement surface. Their exact location along the length of the perimeter may not be known. This can be a strong deterrent to selecting barriers with foundations as a solution. For high-risk buildings, it is recommended that these issues be resolved so that a proper anti-ram solution is worked out and installed.

### Barrier Design Considerations

The effectiveness of a barrier is based on the amount of energy it can absorb versus the amount of kinetic energy,  $KE$ , imparted by a head-on vehicle impact:

$$KE = \frac{Mv^2}{2}$$

where  $M$  is the mass of the vehicle and  $v$  is the velocity at the time of impact with the barrier. The angle of approach reduces this energy in non-head-on situations and the energy absorbed by the crushing of the bumper also reduces the energy imparted to the barriers. Because the velocity is squared in this equation, a change in velocity affects the result more than a change in vehicle weight. For this reason, it is important to review lines of approach to ensure that a vehicle does not have a long, straight road to pick up speed before impact.

The vehicle weight used for the design of barriers typically ranges from 4,000 pounds for cars up to 40,000 pounds for trucks. Impact velocities typically range from 30 mph for slanted impact areas (i.e., where the oncoming street is parallel to the curb) up to 50 mph where there is straight-on access (i.e., where the oncoming street is perpendicular to the curb).

For lower-risk buildings without straight-on vehicular access, it may be more appropriate to install surface mounted systems, such as planters, or use landscaping features to deter an intrusion threat. An example of a simple, but effective, landscaping solution is to install a wide permanent planter around the building with a wall that is as high as a car or truck bumper. Individual planters mounted on the sidewalk resist impact through inertia and friction between the planter and the pavement. It can be expected that the planter will move as a result of the impact. Furthermore, to reduce displacement, the planter may be positioned several inches below the pavement surface. A roughened, grouted surface also will improve performance. The objective is to keep the displacement less than the building setback.

In high security sites and at points where access must be provided through an anti-ram perimeter, active or operational anti-ram systems are required. Off-the-shelf products are available that are rated to resist various levels of car and truck impacts (see Figure 2-14). Solutions include crash beams, crash gates, surface mounted plate systems, retractable bollards, and rotating wedge systems.



Figure 2-14 Examples of active and passive vehicle barriers

The following are some security considerations for sites requiring security measures (see also Sections 2.4.1 and 2.4.2):

- Design and select barriers based on threat capabilities.
- If the limited availability of land precludes the creation of an exclusive zone, the use of screening surrounding the building is an alternative.
- Use a combination of barriers. Some barriers are fixed and obvious (fences and gates), while others are passive (sidewalks far away from buildings, curbs with grassy areas, etc.).
- Where physical barriers are required, consider using landscape materials to create barriers that are soft and natural rather than manmade.
- Vehicles can be used as temporary physical barriers if they are placed in front of buildings or across access roads.

- Maintain as much stand-off distance as possible between potential vehicular bombs and the building:
  - Provide traffic obstacles near entry control points to slow down traffic.
  - Consider vehicle barriers at building entries and drives.
  - Offset vehicle entrances from the direction of a vehicle's approach to force a reduction in speed.
  - When possible, position gates and perimeter boundary fences outside the blast vulnerability envelope.
  - If the threat level warrants, provide a vehicle crash resistance system in the form of a low wall or earth berm.
- Provide passive vehicle barriers to keep stationary vehicle bombs at a distance from the asset.
  - Use high curbs, low berms, shallow ditches, trees, shrubs, and other physical separations to keep stationary bombs at a distance.
  - Do not allow vehicles to park next to perimeter walls of the secured area. Consider using bollards or other devices to keep vehicles away.

## **2.5 ENTRY CONTROL AND VEHICULAR ACCESS**

If a perimeter barrier is employed, it will be necessary to provide points of access through the perimeter for building users (i.e., employees, visitors, and service providers). An entry control point or guard building serves well as the designated point of entry for site access. It provides a point for implementation of desired/required levels of screening and access control; an example is shown in Figure 2-15. The objective of the entry control point is to prevent unauthorized access while maximizing the rate of authorized access by foot or vehicle. These measures are not required for all sites and buildings; they are only required for those considered at high risk.



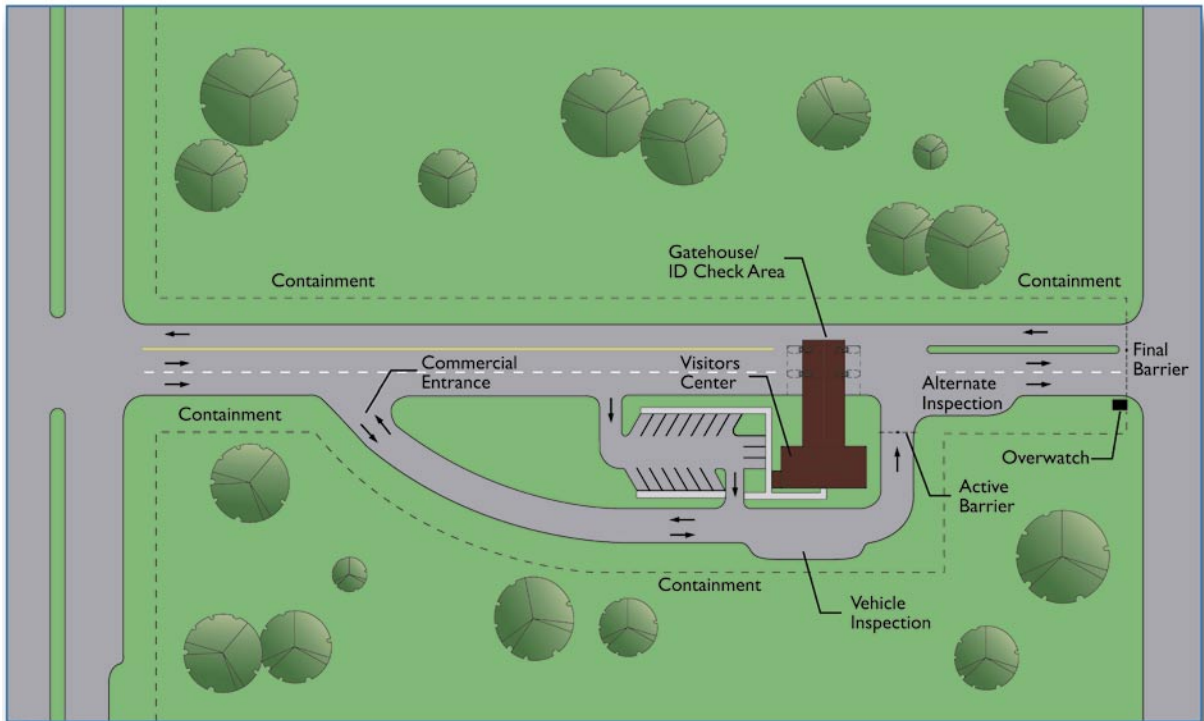


Figure 2-15 Combined multi-user gate

Location selection for vehicular access and entry control for a building starts with an evaluation of the anticipated demand for access to the controlled site. An analysis of traffic origin and destination, and an analysis of the capability of the surrounding connecting road network, including its capacity to handle additional traffic, should then be performed. Expansion capacity should also be considered. The analysis should be coordinated with the state and local departments of transportation.

The existing terrain can have a significant impact on the suitability of a potential entry control point site. Flat terrain with no thick vegetation is generally preferred. A gentle rise in elevation up to the entry control guard building allows for a clear view of arriving vehicles. Consider how existing natural features such as bodies of water or dense tree stands may enhance perimeter security and vehicle containment. Entry control spatial requirements vary, depending on the type, the traffic demand, and the necessary security measures.

In commercial buildings or campuses, more than one type of entry may be required to accommodate the three basic types of traffic (site personnel, visitors, and commercial traffic). Active perimeter entrances should be designated so that security personnel can maintain full control without creating unnecessary delays in traffic. This could be accomplished with a sufficient number of entrances to accommodate the peak flow of pedestrian and vehicular traffic, and adequate lighting for rapid and efficient inspection. Some entrances may be closed during non-peak periods, and should be securely locked, illuminated during hours of darkness, and inspected periodically. Additionally, warning signs should be used to warn drivers when gates are closed. Doors and windows on buildings that form a part of the perimeter should be locked, lighted, and inspected regularly.

The following measures should be considered in the design of entry control points:

- Design entry roads to sites and to individual buildings so that they do not provide direct or straight-line vehicular access to high-risk buildings. Route major corridors away from concentrations of high-risk buildings.
- Design access points at an angle to oncoming streets so that it is difficult for a vehicle to gain enough speed to break through the stations.
- Minimize the number of access roads and entrances into a building or site.
- Designate entry to the site for commercial, service, and delivery vehicles, preferably away from high-risk buildings whenever possible.
- Design the entry control point and guard building so that the authorization of approaching vehicles and occupants can be adequately assessed, and the safety of both gate guards and approaching vehicles can be maintained during periods of peak volume.

- Approach to the site should be designed to accommodate peak traffic demand without impeding traffic flow in the surrounding road network.
- Provide pull-over lanes at site entry gates to check suspect vehicles. When necessary, provide a visitor/site personnel inspection area to check vehicles prior to allowing access to a site or building.
- Design active vehicle crash barriers (e.g., road alignment, retractable bollards, swing gates, or speed bumps) as may be required to control vehicle speed and slow incoming vehicles to give entry control personnel adequate time to respond to unauthorized activities.
- Design the inspection area so that it is not visible to the public, when necessary. Place appropriate landscape plantings to accomplish screening.
- Consider current and future inspection technologies (e.g., above vehicle and under vehicle surveillance systems, ion scanning, and x-ray equipment).
- Provide inspection bays that can be enclosed to protect inspection equipment in the event of bad weather.
- Design inspection areas that are large enough to accommodate a minimum of one vehicle and a pull-out lane. They should also be covered and capable of accommodating the inspection of the undercarriage plus overhead inspection equipment.
- If space is available, provide traffic queuing for vehicles needing authorization.
- Consider providing a walkway and turnstile for pedestrians and a dedicated bicycle lane.
- If possible, provide a gatehouse for the workstations and communications equipment of the security personnel. It may also serve as a refuge in the event of an attack.
- Provide some measure of protection against hostile activity if ID checking is required between the traffic lanes.

- For high security buildings, provide a final denial barrier to stop unauthorized vehicles from entering the site. Most individuals who may attempt to enter without authorization are lost, confused, or inattentive, but there are also those whose intent may be to “run the gate.” A properly designed final denial barrier will take into account both groups, safely stopping the individuals who have made an honest mistake, but providing a properly designed barrier to stop those with hostile intentions.
- Design the barrier system to impede both inbound and outbound vehicles. The system should include traffic control features to deter inbound vehicles from using outbound lanes for unauthorized access. Barrier devices that traverse both roadways should be included in the design. The safety features discussed above for inbound lanes should also be provided in the outbound lanes.

## **2.6 SIGNAGE**

Wayfinding is an important function of design that illustrates the importance of coordination among practitioners and community planning, public works, transportation, law enforcement, and fire-rescue organizations. The ability of users to navigate an unfamiliar environment is important for its success on a day-to-day basis, but will become critical in an emergency situation. In addition to overt prompts such as landmarks, architectural elements, and clear, consistent signage and maps, users will subconsciously rely on cues from their surroundings to help them select a path to safety. Similarly, emergency responders will depend in part on these design elements in order to navigate the scene.

Signs are an important element of security. They are meant to keep intruders out of restricted areas; however, inadequate signs can create confusion and defeat their primary purpose. Confusion over site circulation, parking, and entrance locations can contribute to a loss of site security. Signs should be provided off site and at entrances. There should be on-site directional,



parking, and cautionary signs for visitors, employees, service vehicles, and pedestrians. Unless required, signs should not identify sensitive areas. A comprehensive signage plan should include the following:

- Prepare signs for each entry control building.
- Prepare entry control procedures signs, which explain current entry procedures for drivers and pedestrians.
- Prepare traffic regulatory and directional signs, which control traffic flow and direct vehicles to specific appropriate points.
- Consider using street addresses or building numbers instead of detailed descriptive information inside the site.
- Minimize the number of signs identifying high-risk buildings; however, a significant number of warning signs should be erected to ensure that possible intruders are aware of entry into restricted areas.
- Minimize signs identifying critical utility complexes (e.g., power plants and water treatment plants). Post clear signs to minimize accidental entry by unauthorized personnel into critical asset areas.
- Install warning signs that are easy to understand along the physical barriers and at each entry point.
- Warning signs must use both (or more) languages in areas where two or more languages are commonly spoken. The wording on the signs should denote warning of a restricted area. The signs should be posted at intervals of no more than 100 feet and should not be mounted on fences equipped with intrusion-detection equipment. Additionally, the warning signs should be posted at all entrances to limited, controlled, and exclusion areas.
- Locate variable message signs, which give information on site/organization special events and visitors, far inside site perimeters.

## 2.7 PARKING

Parking restrictions can help to keep potential threats away from a building. In urban settings, however, curbside or underground parking is often necessary and sometimes difficult to control. Mitigating the risks associated with parking requires creative design measures, including parking restrictions, perimeter buffer zones, barriers, structural hardening, and other architectural and engineering solutions. Operational measures may also be necessary to inspect or screen vehicles entering parking garages. The following considerations may help designers to implement sound parking measures for buildings that may be at high risk:

- Locate vehicle parking and service areas away from high-risk buildings to minimize blast effects from potential vehicle bombs.
- Restrict parking from the interior of a group of buildings.
- If possible, locate visitor or general public parking near, but not on, the site itself.
- Restrict parking within the secured perimeter of an asset from unauthorized personnel.
- Locate general parking in areas that present the fewest security risks to personnel.
- If possible, design the parking lot with one-way circulation to facilitate monitoring for potential aggressors.
- Locate parking within view of occupied buildings.
- Prohibit parking within the stand-off zone.
- When establishing parking areas, provide emergency communication systems (e.g., intercom, telephones, etc.) at readily identified, well-lighted, closed circuit television monitored locations to permit direct contact with security personnel.
- Provide parking lots with closed circuit television cameras connected to the security system and adequate lighting capable of displaying and videotaping lot activity.

- Request appropriate permits to restrict parking in curb lanes in densely populated areas to company-owned vehicles or key employee vehicles.
- Provide appropriate setback from parking on adjacent properties if possible. Structural hardening may be required if the setback is insufficient. In new designs, it may be possible to adjust the location of the building on the site to provide adequate setback from adjacent properties.
- If possible, prohibit parking beneath or within a building.
- If parking beneath a building is unavoidable, limit access to the parking areas and ensure they are secure, well-lighted, and free of places of concealment.
- Do not permit uninspected vehicles to park under a building or within the exclusive zone. If parking within the building is required, the following restrictions may be applied:
  - Public parking with ID check
  - Company vehicles and employees of the building only
  - Selected company employees only, or those requiring security
- Apply the following when parking inside a building is necessary and the building superstructure is supported by the parking structure:
  - Protect primary vertical load carrying members by implementing architectural or structural features that provide a minimum 6-inch stand-off from the face of the member.
  - Design columns in the garage area for an “unbraced length” equal to two floors, or three floors where there are two levels of parking.
- For all standalone, aboveground parking garages, maximize visibility for surveillance into, out of, and across the garage.

- Employ express or non-parking ramps, sending the user to parking on flat surfaces.
- Avoid dead-end parking areas, as well as nooks and crannies.
- Design landscaping that does not provide hiding places. It is desirable to locate plantings away from parking garages and parking lots to permit observation of pedestrians.

Additional parking considerations include:

- Stairways and elevator lobby design should be as open as code permits. The ideal solution is a stair and/or elevator waiting area totally open to the exterior and/or the parking areas. Designs that ensure that people using these areas can be easily seen (and can see out) should be encouraged. If a stair must be enclosed for code or weather protection purposes, glass walls can be used to deter potential attacks. Potential hiding places below stairs and within and around stairwells should be closed off.
- Elevator cabs should have glass backs whenever possible. Elevator lobbies should be well-lighted and visible to both patrons in the parking areas and the people outside the building.
- Pedestrian paths should be designed to concentrate activity to the extent possible. For example, bringing all pedestrians through one portal rather than allowing them to disperse to numerous access points improves the ability to see and be seen by other users. Limiting vehicular entry/exits to a minimum number of locations is also beneficial.

## **2.8 LOADING DOCKS AND SERVICE ACCESS**

Loading docks and service access areas are commonly required for a building and are typically desired to be kept as invisible as possible. For this reason, special attention should be devoted to these service areas in order to avoid undesirable intruders. Design criteria for loading docks and service access include the following:

- Separate (by at least 50 feet) loading docks and shipping and receiving areas in any direction from utility rooms, utility

mains, and service entrances, including electrical, telephone/data, fire detection/alarm systems, fire suppression water mains, cooling and heating mains, etc.

- Locate loading docks so that vehicles will not be allowed under the building. If this is not possible, the service should be hardened for blast. Loading dock design should limit damage to adjacent areas and vent explosive forces to the exterior of the building.
- If loading zones or drive-through areas are necessary, monitor them and restrict height to keep out large vehicles.
- Avoid having driveways within or under buildings.
- Significant structural damage to the walls and ceiling of the loading dock may be acceptable; however, the areas adjacent to the loading dock should not experience severe structural damage or collapse. Provide adequate design to prevent extreme damage to loading docks. The floor of the loading dock does not need to be designed for blast resistance if the area below is not occupied and/or does not contain critical utilities.
- Provide signage to clearly mark separate entrances for deliveries.

## **2.9 PHYSICAL SECURITY LIGHTING**

Security lighting should be provided for overall site/building illumination and the perimeter to allow security personnel to maintain visual-assessment during darkness. It may provide both a real and psychological deterrent for continuous or periodic observation. Lighting is relatively inexpensive to maintain and may reduce the need for security personnel by reducing opportunities for concealment and surprise by potential attackers. Lighting is particularly desirable for sensitive areas of a site such as pier and dock areas, vital buildings, storage areas, and vulnerable control points in communications, power, and water distribution systems. It facilitates detection of unauthorized personnel and makes the job of an attacker more difficult.

At entry control points, a minimum surface lighting average of 4 horizontal foot-candles will help ensure adequate lighting for pedestrians, islands, and guards. Where practical, high-mast lighting is recommended, because it gives a broader, more natural light distribution, requires fewer poles (less hazardous to the driver), and is more aesthetically pleasing than standard lighting. Lighting of the entry control point should give drivers a clear view of the gatehouse and, for security personnel, it gives a clear view of the drivers and vehicles.

The type of site lighting system used depends on the overall requirements of the site and the building. Four types of lighting are used for security lighting systems:

- **Continuous lighting** is the most common security-lighting system. It consists of a series of fixed lights arranged to flood a given area continuously during darkness with overlapping cones of light. Two primary methods of using continuous lighting are glare projection and controlled lighting:
  - The glare projection security-lighting method lights the area surrounding a controlled area with high-intensity lighting. It is a strong deterrent to a potential intruder because it makes him or her very visible while making it difficult to see inside the secure area. Guards are protected by being kept in comparative darkness while being able to observe intruders at a considerable distance. This method should not be used when the glare of lights directed across the surrounding territory could annoy or interfere with adjacent operations.
  - Controlled lighting is best when there are limits to the lighted area outside the perimeter, such as along highways. In controlled lighting, the width of the lighted strip is controlled and adjusted to fit the particular need. This method of lighting may illuminate or silhouette security personnel.

- **Standby lighting** has a layout similar to continuous lighting; however, the lights are not continuously lit, but are either automatically or manually turned on when suspicious activity is detected or suspected by security personnel or alarm systems.
- **Movable lighting** consists of manually operated, movable searchlights that may be lit during hours of darkness or as needed. The system normally is used to supplement continuous or standby lighting.
- **Emergency lighting** is a backup power system of lighting that may duplicate any or all of the above systems. Its use is limited to times of power failure or other emergencies that render the normal system inoperative. It depends on an alternative power source such as installed or portable generators or batteries. Consider emergency/backup power for security lighting as determined to be appropriate.

## 2.10 SITE UTILITIES

Utility systems can suffer significant damage when subjected to the shock of an explosion. Some of these utilities may be critical for safely evacuating people from the building. Their destruction could cause damage that is disproportionate to other building damage resulting from an explosion. Additional information on mechanical systems is presented in Section 3.4. To minimize the possibility of such hazards, apply the following measures:

- Where possible, provide underground, concealed, and protected utilities.
- Provide redundant utility systems to support site security, life safety, and rescue functions.
- Consider quick connects for portable utility backup systems if redundant sources are not available.
- Prepare vulnerability assessments for all utility services to the site, including all utility lines, storm sewers, gas transmission

lines, electricity transmission lines, and other utilities that may cross the site perimeter.

- Protect water treatment plants and storage tanks from waterborne contaminants by securing access points, such as manholes. Maintain routine water testing to help detect waterborne contaminants.
- Minimize signs identifying critical utility complexes (e.g., power plants and water treatment plants). Provide fencing to prevent unauthorized access and use landscape planting to conceal aboveground systems.
- Locate petroleum, oil, and lubricant storage tanks and operations buildings downslope from all other buildings. Site fuel tanks at an elevation lower than operational buildings or utility plants. Locate fuel storage tanks at least 100 feet from buildings.
- Locate the main fuel storage away from loading docks, entrances, and parking. Access should be restricted and protected (e.g., locks on caps and seals).
- Provide utility systems with redundant or loop service, particularly in the case of electrical systems. Where more than one source or service is not currently available, provisions should be made for future connections. In the interim, consider “quick connects” at the building for portable backup systems.
- Decentralize a site’s communications resources when possible; the use of multiple communications networks will strengthen the communications system’s ability to withstand the effects of a terrorist attack. Careful consideration should be made in locating, concealing, and protecting key network resources such as network control centers.
- Place trash receptacles as far away from the building as possible; trash receptacles should not be placed within 30 feet of a building.
- Conceal incoming utility systems within building and property lines, and give them blast protection, including burial or proper encasement, wherever possible.



- Consider incorporating low impact development practices to enhance security, such as retaining stormwater on site in a pond to create stand-off, instead of sending into the sewer system.
- Locate utility systems at least 50 feet from loading docks, front entrances, and parking areas.
- Route critical or fragile utilities so that they are not on exterior walls or on walls shared with mailrooms.
- Where redundant utilities are required in accordance with other requirements or criteria, ensure that the redundant utilities are not collocated or do not run in the same chases. This minimizes the possibility that both sets of utilities will be adversely affected by a single event.
- Where emergency backup systems are required, ensure they are located away from the systems components for which they provide backup.
- Mount all overhead utilities and other fixtures weighing 31 pounds (14 kilograms) or more to minimize the likelihood that they will fall and injure building occupants. Design all equipment mountings to resist forces of 0.5 times the equipment weight in any direction and 1.5 times the equipment weight in the downward direction. This standard does not preclude the need to design equipment mountings for forces required by other criteria such as seismic standards.
- To limit opportunities for aggressors placing explosives underneath buildings, ensure that access to crawl spaces, utility tunnels, and other means of under building access is controlled.

All utility penetrations of a site's perimeter barrier, including penetrations in fences, walls, or other perimeter structures, should be sealed or secured to eliminate openings large enough to pass through the barrier. Typical penetrations could be for storm sewers, water, electricity, or other site

utility services. Specific requirements of various openings are discussed below:

- All utility penetrations of the site's perimeter should be screened, sealed, or secured to prevent their use as access points for unauthorized entry into the site. If access is required for maintenance of utilities, secure all penetrations with screening, grating, latticework, or other similar devices so that openings do not allow intruder access. Provide intrusion detection sensors and consider overt or covert visual surveillance systems if warranted by the sensitivity of assets requiring protection.
- Drainage ditches, culverts, vents, ducts, and other openings that pass through a perimeter and that have a cross-sectional area greater than 96 square inches and whose smallest dimension is greater than 6 inches should be protected by securely fastened welded bar grilles. As an alternative, drainage structures may be constructed of multiple pipes, with each pipe having a diameter of 10 inches or less. Multiple pipes of this diameter may also be placed and secured in the inflow end of a drainage culvert to prevent intrusion into the area. Ensure that any addition of grills or pipes to culverts or other drainage structures is coordinated with the engineers so that they can compensate for the diminished flow capacity and additional maintenance that will result from the installation.
- Manhole covers 10 inches or more in diameter must be secured to prevent unauthorized opening. They may be secured with locks and hasps, by welding them shut, or by bolting them to their frame. Ensure that hasps, locks, and bolts are made of materials that resist corrosion. Keyed bolts (which make removal by unauthorized personnel more difficult) are also available. If very high security is required, manhole covers that resist shattering after being artificially "frozen" by an aggressor should be considered.

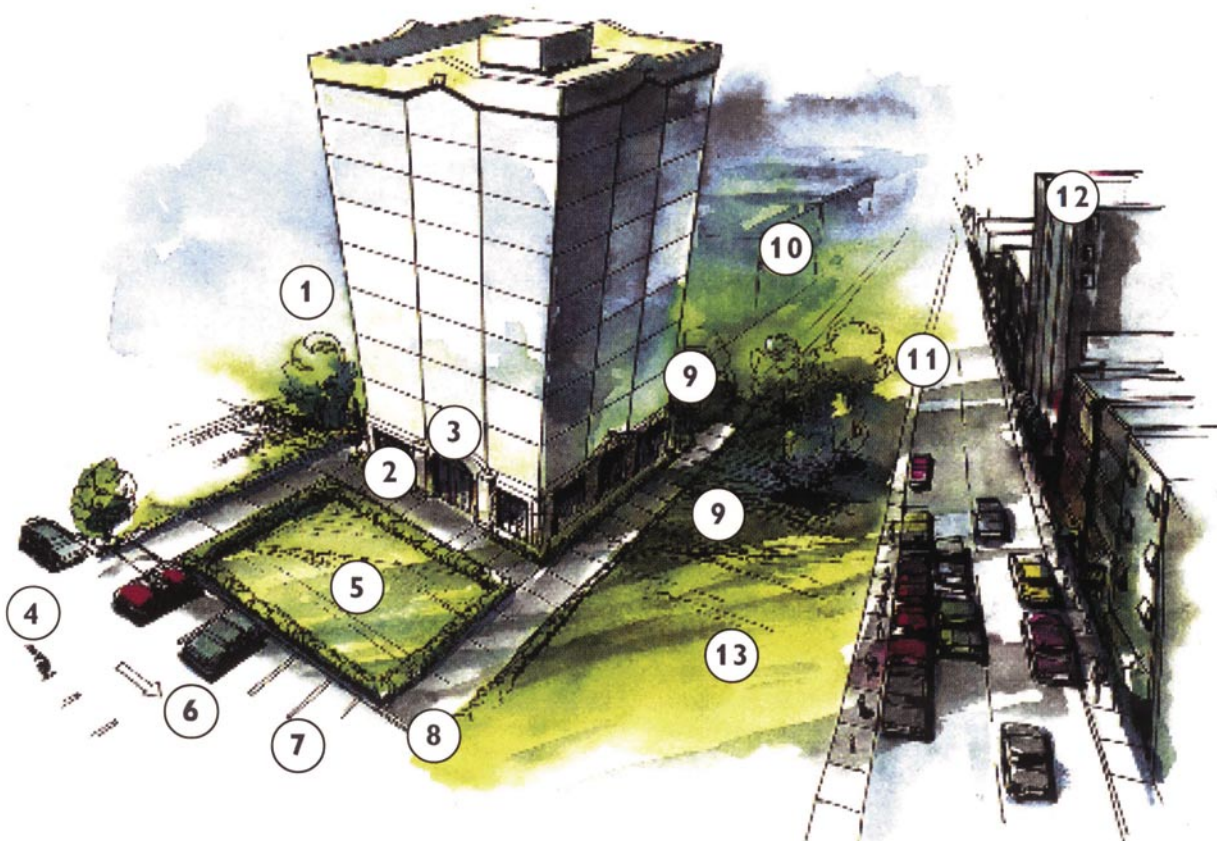
## **2.1 1 SUMMARY OF SITE MITIGATION MEASURES**

A general spectrum of site mitigation measures ranging from the least protection, cost, and effort going to the greatest protection, cost, and effort is presented below. Detailed discussions of individual measures can be found earlier in the chapter. This is a nominal ranking of mitigation measures. In practice, the effectiveness and cost of individual mitigation measures may be different for specific applications. Figure 2-16 is a graphic summary of site mitigation measures to protect building occupants. Table 2-1 correlates mitigation measures to specific threats.

**Less Protection  
Less Cost  
Less Effort**

- Place trash receptacles as far away from the building as possible.
- Remove any dense vegetation that may screen covert activity.
- Use thorn-bearing plant materials to create natural barriers.
- Identify all critical resources in the area (fire and police stations, hospitals, etc.).
- Identify all potentially hazardous facilities in the area (nuclear plants, chemical labs, etc.).
- Use temporary passive barriers to eliminate straight-line vehicular access to high-risk buildings.
- Use vehicles as temporary physical barriers during elevated threat conditions.
- Make proper use of signs for traffic control, building entry control, etc. Minimize signs identifying high-risk areas.
- Identify, secure, and control access to all utility services to the building.
- Limit and control access to all crawl spaces, utility tunnels, and other means of under building access to prevent the planting of explosives.
- Utilize Geographic Information Systems (GIS) to assess adjacent land use.
- Provide open space inside the fence along the perimeter.
- Locate fuel storage tanks at least 100 feet from all buildings.
- Block sight lines through building orientation, landscaping, screening, and landforms.
- Use temporary and procedural measures to restrict parking and increase stand-off.
- Locate and consolidate high-risk land uses in the interior of the site.
- Select and design barriers based on threat levels.
- Maintain as much stand-off distance as possible from potential vehicle bombs.
- Separate redundant utility systems.
- Conduct periodic water testing to detect waterborne contaminants.
- Enclose the perimeter of the site. Create a single controlled entrance for vehicles (entry control point).
- Establish law enforcement or security force presence.
- Install quick connects for portable utility backup systems.
- Install security lighting.
- Install closed circuit television cameras.
- Mount all equipment to resist forces in any direction.
- Include security and protection measures in the calculation of land area requirements.
- Design and construct parking to provide adequate stand-off for vehicle bombs.
- Position buildings to permit occupants and security personnel to monitor the site.
- Do not site the building adjacent to potential threats or hazards.
- Locate critical building components away from the main entrance, vehicle circulation, parking, or maintenance area. Harden as appropriate.
- Provide a site-wide public address system and emergency call boxes at readily identified locations.
- Prohibit parking beneath or within a building.
- Design and construct access points at an angle to oncoming streets.
- Designate entry points for commercial and delivery vehicles away from high-risk areas.
- In urban areas, push the perimeter out to the edge of the sidewalk by means of bollards, planters, and other obstacles. For better stand-off, push the line farther outward by restricting or eliminating parking along the curb, eliminating loading zones, or through street closings.
- Provide intrusion detection sensors for all utility services to the building.
- Provide redundant utility systems to support security, life safety, and rescue functions.
- Conceal and/or harden incoming utility systems.
- Install active vehicle crash barriers.

**Greater  
Protection  
Greater Cost  
Greater Effort**



1. Locate assets stored on site, but outside the building within view of occupied rooms in the facility.	8. Minimize vehicle access points.
2. Eliminate parking beneath buildings.	9. Eliminate potential hiding places near the building; provide an unobstructed view around building.
3. Minimize exterior signage or other indications of asset locations.	10. Site building within view of other occupied buildings on the site.
4. Locate trash receptacles as far from the building as possible.	11. Maximize distance from the building to the site boundary.
5. Eliminate lines of approach perpendicular to the building.	12. Locate building away from natural or manmade vantage points.
6. Locate parking to obtain stand-off distance from the building.	13. Secure access to power/heat plants, gas mains, water supplies, and electrical service.
7. Illuminate building exteriors or sites where exposed assets are located.	

Figure 2-16 Summary of site mitigation measures

Table 2-1: Correlation of Mitigation Measures to Threats\*

	<div> <div> <div></div> <div>The symbols indicate which of the protective measures shown in the left-hand column can be effective in countering the types of threats indicated across the top of the chart.</div> </div> </div>								
	Moving Vehicle Bomb	Stationary Vehicle Bomb	Exterior Attack	Stand-off Weapons Attack	Armed Attack	Covert Entry	Mail and Supplies Bombs	Airborne Contamination	Waterborne Contamination
<b>LAND USE CONSIDERATIONS</b>									
Locate high-risk land uses in the interior of the site	■	■	■	■	■				
Consolidate high-risk land uses	■	■	■	■	■				
Include stand-off areas in land area requirements	■	■		■	■				
Consider effects of off-property development	■	■	■		■				
<b>SITE PLANNING</b>									
Maximize distance from perimeter fence and developed areas	■	■	■	■	■			■	
Site critical facilities on higher ground	■	■	■	■	■			■	■
Avoid areas with adjacent high terrain or structures			■	■	■			■	■
Avoid areas with adjacent dense vegetation			■	■	■				
Avoiding low-lying topographic areas			■	■	■			■	■
Provide separation between facilities	■	■	■	■	■		■		
Site facilities within view of other occupied facilities						■			
Cluster facilities with similar threat levels	■	■		■	■				
Create complexes to enhance surveillance opportunities	■	■	■	■	■				
Eliminate vehicle parking from interior of building complexes	■	■							
High surrounding terrain			■	■	■				
Distance from non-building facilities	■	■	■	■	■	■		■	■
Areas that provide concealment		■	■	■	■	■			

Table 2-1: Correlation of Mitigation Measures to Threats\* (continued)

	Moving Vehicle Bomb	Stationary Vehicle Bomb	Exterior Attack	Stand-off Weapons Attack	Armed Attack	Covert Entry	Mail and Supplies Bombs	Airborne Contamination	Waterborne Contamination
Earth berms		■	■	■	■				
Bodies of water	■	■	■	■	■	■			
Depressions			■	■	■				
Protect against unwanted surveillance			■	■	■	■			
"Defensible space"		■	■			■			
Vehicle access	■	■							
Dense thorn-bearing vegetation			■			■			
Vegetation screens		■	■	■	■	■			
Location of trash receptacles							■		
<b>STAND-OFF DISTANCE</b>									
Stand-off zone	■	■		■	■	■			
<b>CONTROLLED ACCESS ZONES</b>									
Exclusive zone/Non-exclusive zone	■	■				■			
Clear zone	■	■				■			
Fencing and physical barriers	■	■	■	■	■	■			
Active barriers	■	■	■	■	■	■			
Passive barriers	■	■	■			■			
<b>ENTRY CONTROL AND VEHICULAR ACCESS</b>									
Minimize access roads	■	■				■	■		
Control points	■	■	■	■	■	■			

Table 2-1: Correlation of Mitigation Measures to Threats\* (continued)

	Moving Vehicle Bomb	Stationary Vehicle Bomb	Exterior Attack	Stand-off Weapons Attack	Armed Attack	Covert Entry	Mail and Supplies Bombs	Airborne Contamination	Waterborne Contamination
Active monitoring	■	■	■	■	■	■	■	■	■
Provide enhanced protection at property entrances	■	■	■	■	■	■			
Include pull-over lanes at checkpoints to inspect vehicles	■	■	■	■	■	■			
Avoid straight-line vehicular access to high-risk resources	■	■							
Avoid straight-line entry approach roads	■	■							
Locate vehicle parking areas far from high-risk resources	■	■							
Provide separate service and delivery access	■	■							
Route major corridors away from high-risk resources	■	■		■	■				
Locate high-risk resources remote from primary roads	■	■		■	■				
Minimize directional identification signs	■	■	■	■	■	■			
Limit vehicular access to high-risk resources	■	■	■	■	■	■			
<b>SIGNAGE</b>									
Minimize signage	■	■	■	■	■	■	■	■	■
<b>PARKING</b>									
View of parking		■							
Parking under a building		■							
Parking at interior of facility		■							
Parking near high-risk areas		■							



Table 2-1: Correlation of Mitigation Measures to Threats\* (continued)

	Moving Vehicle Bomb	Stationary Vehicle Bomb	Exterior Attack	Stand-off Weapons Attack	Armed Attack	Covert Entry	Mail and Supplies Bombs	Airborne Contamination	Waterborne Contamination
Parking in exclusive zone		■							
One-way circulation	■	■	■			■			
<b>LOADING DOCKS AND SERVICE ACCESS</b>									
Loading/unloading docks		■					■		
Driveways under facilities	■	■							
<b>PHYSICAL SECURITY LIGHTING</b>									
Lighting		■	■			■			
<b>SITE UTILITIES</b>									
Provide protection at culverts, sewers, and pipelines					■	■			■
Provide protection at concrete trenches, storm drains, and duct systems					■	■			■
Provide and check locks on manhole covers					■	■			■
Minimize signs identifying utility systems					■	■			■
Provide fencing at critical utility complexes						■			■
Use landscape planting to conceal aboveground systems						■			■
Install utilities underground	■	■	■	■	■	■	■		
Locate fuel/lube storage downslope and away from facilities	■	■	■	■	■	■	■		
Provide redundant utility systems and loop service	■	■	■	■	■	■	■		
Provide utility "quick disconnects" for portable backup systems	■	■	■	■	■	■	■		

Table 2-1: Correlation of Mitigation Measures to Threats\* (continued)

	Moving Vehicle Bomb	Stationary Vehicle Bomb	Exterior Attack	Stand-off Weapons Attack	Armed Attack	Covert Entry	Mail and Supplies Bombs	Airborne Contamination	Waterborne Contamination
Decentralize communications resources	■	■	■	■	■	■	■		
Use multiple communications networks	■	■	■	■	■	■	■		
Conceal and protect network control centers	■	■	■	■	■	■	■		
Public address system			■		■			■	■
Underground utilities	■	■	■	■					■
Redundant utilities	■	■	■	■	■				■
Quick disconnects	■	■	■	■	■				
Remote fuel storage	■	■	■	■	■				

\* Adapted from U.S. Air Force, *Installation Force Protection Guide*.

## **2.12 CRIME PREVENTION THROUGH ENVIRONMENTAL DESIGN (CPTED)**

CPTED is a crime reduction technique that has several key elements applicable to the analysis of building function and site design against physical attack. It is used by architects, city planners, landscape and interior designers, and law enforcement with the objective of creating a climate of safety in a community by designing a physical environment that positively influences human behavior. Although CPTED principles are not incorporated into the assessment process presented herein, it is useful to briefly discuss CPTED because it is often entwined with terrorism protection measures. Indeed, many antiterrorist design approaches are similar to those found in CPTED.

CPTED concepts have been successfully applied in a wide variety of applications, including streets, parks, museums, government buildings, houses, and commercial complexes. The approach is particularly applicable to older buildings that were designed and constructed 30 to 60 or more years ago. Security issues were almost nonexistent at the time, and technology was dramatically different. As a result, building designs are not always compatible with today's more security-conscious environment.

According to CPTED principles, depending upon purely conventional physical security measures (e.g., security guards and metal detectors) to correct objectionable behavior may have its limitations. Although employing these measures will no doubt increase the level of physical security, in some cases physical security measures employed as standalone actions may lead to a more negative environment, thereby enhancing violence. In short, employing standalone physical security measures may fail to address the underlying behavioral patterns that adversely affect the particular environment. CPTED analysis focuses on creating changes to the physical and social environment that will reinforce positive behavior.

CPTED builds on three strategies:

- Territoriality (using buildings, fences, pavement, signs, and landscaping to express ownership)
- Natural surveillance (placing physical features, activities, and people to maximize visibility)
- Access control (the judicious placement of entrances, exits, fencing, landscaping, and lighting)

A CPTED analysis of a building evaluates crime rates and stability, as well as core design shortcomings of the physical environment (e.g., blind hallways, uncontrolled entries, or abandoned areas that attract problem behavior). The application of CPTED principles starts with a threat and vulnerability analysis to determine the potential for attack and what needs to be protected. Protecting a building from physical attack by criminal behavior or terrorist activity, in many cases, only reflects a change in the level and types of threats. The CPTED process asks questions about territoriality, natural surveillance, and access control that can:

- Increase the effort to commit crime or terrorism
- Increase the risks associated with crime or terrorism
- Reduce the rewards associated with crime or terrorism
- Remove the excuses as to why people do not comply with the rules and behave inappropriately

The CPTED process provides direction to solve the challenges of crime and terrorism with organizational (people), mechanical (technology and hardware), and natural design (architecture and circulation flow) methods.

CPTED concepts can be integrated into expansion or reconstruction plans for existing buildings as well as new buildings. Applying CPTED concepts from the beginning usually has minimal impact on costs, and the result is a safer building. Each

building, facility, and community should institute measures appropriate for their own circumstances because there is no single solution that will fit all situations.

Many CPTED crime prevention techniques for a building complement conventional terrorism and physical attack prevention measures. For example, as part of the CPTED strategy of improving territoriality, buildings are encouraged to direct all visitors through one entrance that offers contact with a receptionist who can determine the purpose of the visit and the destination, and provide sign-in/sign-out sheets and an identification tag prior to building access. These CPTED measures are similar to and complement physical security entry control point stations.

However, in some cases, CPTED techniques can conflict with basic physical security principles. The CPTED strategy of natural surveillance calls for locating parking in areas that allow ease of monitoring. A design that locates parking close to a building or office also reduces vehicle stand-off and could create a vulnerability of the building structure to a vehicle bomb. In cases where CPTED techniques conflict with security principles, designers should seek innovative solutions tailored to the unique situation.



**T**his chapter addresses explosive blast and CBR concerns from terrorist attacks, highlighting mitigation measures that may be applied to building elements, including architectural, structural, and building envelope systems. After the site design considerations to enhance protection presented in Chapter 2 have been taken into account (recognizing that many may not be applicable to buildings in urban settings), additional building design measures, such as hardening, must be considered to protect building occupants. That is, when the desired level of protection cannot be achieved through site design, building envelope design measures must be considered. Catastrophic collapse of the building is a primary concern. Historically, the majority of fatalities that occur in terrorist attacks directed against buildings are due to building collapse. This was true for the Oklahoma City bombing in 1995 when 87 percent of the building occupants who were killed were in the collapsed portion of the Murrah Federal Building; however, other threats such as CBR agents should also be considered.

When considering mitigation measures for explosive blast threats, the primary strategy is to keep explosive devices as far away from the building as possible (maximize stand-off distance). This is usually the easiest and least costly way to achieve a desired level of protection. In cases where sufficient stand-off distance is not available to protect the building, hardening of the building's structural systems may be required, as well as design to prevent progressive collapse. In addition, designers should try to minimize hazardous flying debris during an explosive event because a high number of injuries can result from flying glass fragments and debris from walls, ceilings, and non-structural features. The hardening of the building envelope should be balanced so that the columns, walls, and windows have approximately equal response for damage and injury/casualty for the design basis threat weapon at the available stand-off distance. Window design is the element that is usually the most diverse in conventional construction. Good blast engineering is a multi-disciplinary effort that requires the concerted

efforts of the architect, structural engineer, mechanical engineer, and the other design team members in order to achieve a balanced building envelope.

When considering mitigation measures for CBR hazards, the HVAC systems are of particular concern. A building can provide protection against CBR agents released outdoors if the flow of fresh air is filtered or interrupted; however, HVAC systems can also become an entry point and distribution system for hazardous contaminants. If installed, HVAC air filtration and air-cleaning systems can reduce the effects of a CBR agent by removing the contaminants from the air within a building. There are a variety of ways to protect building occupants from airborne hazards. These protective measures can be as simple as defining a protective action plan or as complex as strict design measures practical only for new construction.

Building design should be optimized to facilitate emergency evacuation, rescue, and recovery efforts through effective placement, structural design, and redundancy of emergency exits and critical mechanical/electrical systems. Through effective structural design, the overall damage levels may be reduced to make it easier for people to get out safely and allow emergency responders to enter safely. The designer must also balance measures to protect people with the requirements of the ADAAG, UFAS, NFPC, and all applicable local building codes.

The primary focus of this chapter is the protection of buildings where the occupants are the primary asset. In this case, the objective of the designer is to save lives by mitigating building damages and reducing the chances of catastrophic collapse of the building, at least until the building is fully evacuated. The measures described in this chapter are designed to minimize the loss of life through deterrence and detection, as well as strengthening of the building against a variety of terrorist tactics. The design team must determine which measures are appropriate and cost-effective for incorporation into the building design. The measures presented here are not all-inclusive, and additional technical information for implementation can be found in the referenced documents.



### 3.1 ARCHITECTURAL

A lot can be done architecturally to mitigate the effects of a terrorist bombing on a facility. These measures often cost nothing or very little if implemented early in the design process. Architectural considerations include building configuration, space design, and building detailing. It is recommended that architects be brought into the design process as early as site selection, to optimize the protection provided. FEMA 430 contains an expanded discussion of incorporating security components in architectural design.

#### 3.1.1 Building Configuration

The vertical or horizontal profile of a building has implications for its protection. As with the discussion of clustered versus dispersed buildings, designers should balance a number of relevant considerations to the extent that site, economic, and other factors allow. Some of the relevant considerations include the following:

##### Low, Large-footprint Buildings:

- Distribute people, assets, and operations across a wider area, to limit damage
- Use vegetation, terrain, and other screening elements to protect from hostile surveillance
- Maximize the benefits of green roof technologies, which can help reduce a building's heat signature and lower its visual profile

#### Leadership in Energy and Environmental Design (LEED)

As with CPTED, some of the Leadership in Energy and Environmental Design (LEED) concepts complement security concerns and others conflict with physical security principles. The LEED Green Building Rating System represents the U.S. Green Building Council's (USGBC's) effort to provide a national standard for what constitutes a "green building." Through its use as a design guideline and third-party certification tool, it aims to improve occupant well-being, environmental performance, and economic returns of buildings using established and innovative practices, standards, and technologies.<sup>1</sup> LEED is a voluntary building assessment tool that is most applicable to commercial, institutional, and high-rise residential construction. Owners, architects, and engineers must work together to strike a balance between building design objectives.

LEED looks at six basic categories: Sustainable Sites, Water Efficiency, Energy and Atmosphere, Materials and Resources, Indoor Environmental Quality, and Innovation and Design Process. Within each category, points are awarded for achieving specific goals. A total of 69 points is possible. A score of 26-32 points achieves basic certification; 33-38 achieves Silver; 39-51 achieves Gold; and 52-69 points achieve Platinum certification. The LEED rating is awarded after the project has been documented by the USGBC.

Another goal in the LEED effort is to encourage more sustainable construction practices. LEED encourages manufacturers to provide materials that:

- contain high recycled content and sustainable use raw materials
- are manufactured close to the construction site
- have low volatile organic compound emissions
- are designed to minimize energy consumption and packaging

<sup>1</sup> U.S. Green Building Council, *LEED Green Building Rating System for New Construction & Major Renovations Version 2.1*, November 2002. <http://www.usgbc.org>

- Require the use of additional measures (at additional cost) to prevent introduction of CBR agents due to easier access to HVAC intakes by intruders

**Tall, Small-footprint Buildings:**

- Suffer damage to a greater percentage of their façades, structures, and interiors at best, and catastrophic damage or collapse at worst, should a large blast occur near the building if not constructed with progressive collapse prevention in mind
- Elevate occupied areas above vegetation, terrain, and other screening elements, making it potentially more difficult to protect interior spaces from outside surveillance
- Minimize the amount of impervious surface, contributing to a reduction in stormwater runoff, which reduces the need for culverts, drainage pipes, manholes, and other covert site access and weapon concealment opportunities
- Provide greater opportunity to elevate HVAC intakes to prevent the introduction of CBR agents

The shape of the building may also contribute to the overall damage to the structure. For example, “U” or “L” shaped buildings tend to trap shock waves, which may exacerbate the effect of explosive blasts. For this reason, it is recommended that re-entrant corners be avoided. In general, convex rather than concave shapes are preferred for the exterior of the building. For example, circular buildings act to reduce the air-blast pressures because the angle of incidence of the shock wave increases more rapidly than in a rectangular building. The following design considerations are recommended:

- Reduce a building’s vulnerability to attack by using earth-sheltered design
- Orient buildings horizontally rather than vertically to reduce the building’s profile and exposure
- Place the ground floor elevation of a building at 4 feet above grade to prevent vehicle ramming

- Avoid eaves and overhangs, because they can be points of high local pressure and suction during blasts; when these elements are used, they should be designed to withstand blast effects
- Orient glazing perpendicular to the primary facade to reduce exposure to blast and projectiles (see Figure 3-1)

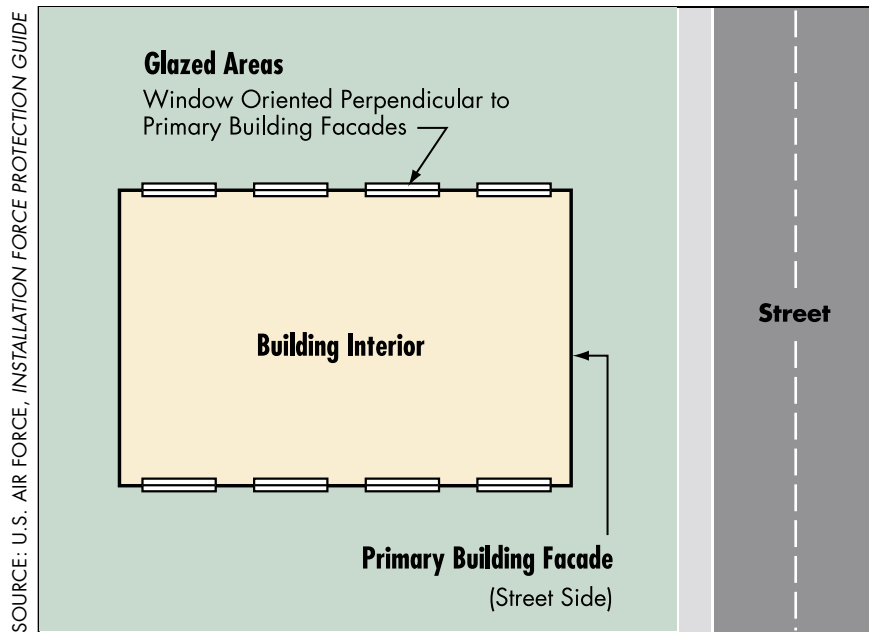


Figure 3-1 Glazed areas perpendicularly oriented away from streets

- Avoid exposed structural elements (e.g., columns) on the exterior of the facility
- Provide pitched roofs to allow deflection of launched explosives
- Avoid re-entrant corners on the building exterior where blast pressures may build up (see Figure 3-2)

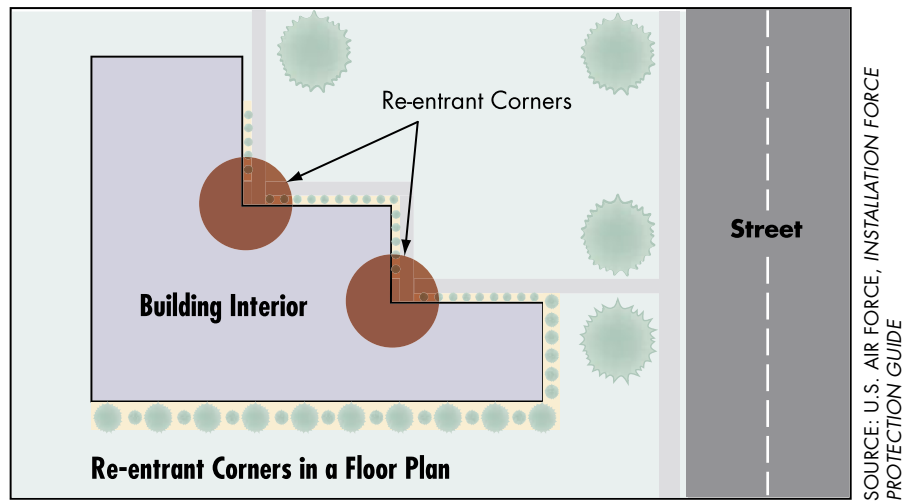


Figure 3-2 Re-entrant corners in a floor plan

### 3.1.2 Space Design

Unsecured areas should be physically separated from the main building to the extent possible. For example, a separate lobby pavilion or loading dock outside the main footprint provides enhanced protection against damages and potential building collapse in the event of an explosion. Similarly, placing parking areas outside the main footprint of the building can be highly effective in reducing the vulnerability to catastrophic collapse.

The protection of the building interior can be divided into two categories: functional layout and structural layout. In terms of functional layout, public areas such as the lobby, loading dock, mail room, garage, and retail areas need to be separated from the more secured areas of the facility. This can be done by creating internal “hard lines” or buffer zones, using secondary stairwells, elevator shafts, corridors, and storage areas between public and secured areas.

In lobby areas, the architect would be wise to consider the queuing requirements in front of the inspection stations so that visitors are not forced to stand outside during bad weather conditions or in a congested line inside a small lobby while waiting to enter the secured areas.

Emergency functions (e.g., sprinkler systems and generators, which are critical for mitigating the effects of an explosion) and elevator shafts should be placed away from internal parking areas and loading docks. In the 1993 World Trade Center bombing incident, elevator shafts became chimneys, transmitting smoke and heat from the explosion in the basement to all levels of the building. This hindered evacuation and caused smoke inhalation injuries. When it is not possible to separate mechanical areas and parking, the walls need to be designed to resist explosive forces. The following design measures should be considered:

- Do not collocate high-risk facilities with lower risk tenants. For example, a post office or supply center/room should not be located in the same building as a childcare facility.
- Locate key assets as far into the interior of a building as possible.
- Place areas of high visitor activity away from key assets.
- Locate critical assets in spaces that are occupied 24 hours per day.
- Locate assets in areas where they are visible to more than one person.
- Eliminate hiding places within the building.
- Use interior barriers to differentiate levels of security within a building.
- Stagger doors located across from one another in interior hallways to limit the effects of a blast through a structure (see Figure 3-3).
- Provide foyers with reinforced concrete walls, and offset interior and exterior doors.
- Consider methods to facilitate the venting of explosive forces and gases from the interior spaces to the

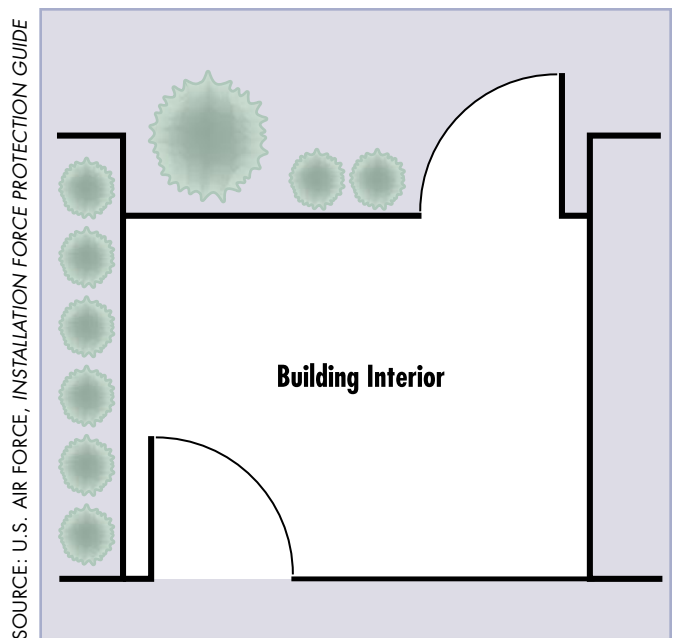


Figure 3-3 Offset doors through foyer

outside of the structure. Examples of such methods include the use of blow-out panels and window system designs that provide protection from blast pressure applied to the outside, but that readily fail and vent if exposed to blast pressure on the inside.

- Physically isolate lobbies, mailrooms (includes various mail processing areas), loading docks, and other entry and storage areas from the rest of the building. These are areas where bulk quantities of CBR agents are likely to enter a building. Building doors, including vestibule and loading dock doors, should remain closed when not in use.
- Design buildings so that lobbies, mailrooms, and loading docks do not share a return-air system or return pathway (e.g., ceiling plenum) with other areas of the building. Some of these measures are more feasible for new construction or buildings undergoing major renovation.

### 3.1.3 Other Design Considerations

When designing high-risk buildings, engineers and architects should consider the following:

- **Safe havens.** The innermost layer of protection within a physical security system is the safe haven. Safe havens are not intended to withstand a disciplined, paramilitary attack featuring explosives and heavy weapons. The safe haven should be designed such that the time attackers need to penetrate the protected area is greater than the time that first responders need to reach the protected area. For additional information on safe havens, see FEMA 428, *Primer to Design Safe School Projects in Case of Terrorist Attacks*.
- **Office locations.** Offices considered to be high risk (more likely to be targeted by terrorists) should be placed or glazed so that the occupants cannot be seen from an uncontrolled public area such as a street. Whenever possible, these spaces should face courtyards, internal sites, or controlled areas. If this is not possible, suitable obscuring glazing or window treatment should be provided, including ballistic-resistant glass, blast curtains, or other interior protection systems.

- **Mixed occupancies.** High-risk tenants should not be housed with low-risk tenants. Terrorists may identify some targets based on their symbology, visibility, ideology, political views, potential for publicity, or simply the consequences of their loss.
- **Public toilets and service areas.** Public toilets, service spaces, or access to vertical circulation systems should not be located in any non-secure areas, including the queuing area before visitor screening at the public entrance.
- **Retail uses in the lobby.** Retail and other mixed uses, which have been encouraged in public buildings by the Public Buildings Cooperative Use Act of 1976, create spaces that are open and inviting. Although important to the public nature of the buildings, the presence of retail and other mixed uses may present a risk to buildings and their occupants and should be carefully considered on a project-specific basis during project design. In areas exposed to potential terrorist attacks, retail and mixed uses may be accommodated through such means as separating entryways, controlling access, and hardening shared partitions, as well as with special security operational countermeasures.
- **Stairwells.** Stairwells required for emergency egress should be located as remotely as possible from areas where blast events might occur and, wherever possible, should not discharge into lobbies, parking, or loading areas.
- **Mailroom.** The mailroom should be located away from facility main entrances areas containing critical services, utilities, distribution systems, and important assets. In addition, the mailroom should be located at the perimeter of the building with an outside wall or window designed for pressure relief. It should have adequate space for explosive disposal containers. An area near the loading dock is a preferred mailroom location. Where these rooms are located in occupied areas or adjacent to critical utilities, walls, ceilings, and floors, they should be blast- and fragment-resistant. Significant structural damage to the walls, ceilings, and floors of the mailroom is acceptable; however, the areas adjacent to the mailroom should not experience severe damage or collapse.

- **Non-structural elements.** False ceilings, light fixtures, venetian blinds, ductwork, air conditioners, and other equipment may become flying debris in the event of an explosion. Wherever possible, it is recommended that the design be simplified to limit these hazards. Placing heavy equipment such as air conditioners near the floor rather than the ceiling is one idea; using curtains rather than venetian blinds, and using exposed ductwork as an architectural device are others.

## **3.2 BUILDING STRUCTURAL AND NON-STRUCTURAL SYSTEMS**

### **3.2.1 Building Design to Achieve a Desired Protection Level**

The assessment process described in Chapter 1 determines the level of protection sought for the building structure and defines the threat/hazard specific to the facility. Explosive blast threats usually govern building structural design for high-risk buildings. A structural engineer should determine the building design features needed to achieve the desired level of protection against the design blast threat, considering collapse of the building, as well as incipient injuries and fatalities. In addition, Chapter 4 discusses other structural systems related to explosive blast.

### **3.2.2 Progressive Collapse**

Progressive collapse is a situation where local failure of a primary structural component leads to the collapse of adjoining members, which, in turn, leads to additional collapse. Hence, the total damage is disproportionate to the original cause. Progressive collapse is a chain reaction of structural failures that follows from damage to a relatively small portion of a structure. Information on progressive collapse can also be found in FEMA 427, *Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks*.

All buildings should be designed with the intent of reducing the potential for progressive collapse as a result of an abnormal loading event, regardless of the required level of protection. The following



structural characteristics (from *GSA Progressive Collapse Analysis and Design Guidelines for New Federal Office Buildings and Major Modernization Projects*, November 2000) should be considered in the initial phases of structural design. Incorporation of these features will provide a more robust structure and decrease the potential for progressive collapse. Designers should consider the following:

- **Redundancy.** The use of redundant lateral and vertical force resisting systems is highly encouraged when considering progressive collapse. Redundancy tends to promote a more robust structure and helps to ensure that alternate load paths are available in the case of a structural element(s) failure. Additionally, redundancy provides multiple locations for yielding to occur, which increases the probability that damage will be constrained.
- **The use of ductile structural elements and detailing.** It is critical that both the primary and secondary structural elements be capable of deforming well beyond the elastic limit, without experiencing structural collapse. The use of ductile construction materials (i.e., steel, cast-in-place reinforced concrete, etc.) for both the structural elements and connection detailing is encouraged. The capability of achieving a ductile response is imperative when considering an extreme redistribution of loading such as that encountered in structural element(s) failure.
- **Capacity for resisting load reversals.** Both the primary and secondary structural elements should be designed to resist load reversals in case of a structural element(s) failure.
- **Capacity for resisting shear failure.** Primary structural elements maintain sufficient strength and ductility under an abnormal loading event to preclude a shear failure. If the shear capacity is reached before flexural capacity, the sudden, non-ductile failure of the element could potentially lead to a progressive collapse of the structure.

Both the GSA and DoD take a threat-independent approach to progressive collapse. The goal of a threat-independent approach

is not to prevent collapse from a specific design threat, but to control and stop the continuing spread of damage after localized damage or localized collapse has occurred.

The GSA and DoD require that the structural response of a building be analyzed in a test that removes a key structural element (e.g., vertical load carrying column, section of bearing wall, beam, etc.) to simulate local damage from an explosion. If effective alternative load paths are available for redistributing the loads, originally supported by the removed structural element, the building has a low potential for progressive collapse. The details of the GSA and DoD guidelines and criteria can be found in *GSA Progressive Collapse Analysis and Design Guidelines for New Federal Office Buildings and Major Modernization Projects* (November 2000) and *DoD Unified Facilities Criteria (UFC) 4-010-01* (31 July 2002). Although these criteria provide specific guidance on which structural elements must be analyzed for removal from the structural design configuration, they do not provide specific guidance for choosing an engineering structural response model for verifying the effectiveness of alternate load paths.

Several other design codes and guidelines in use throughout the world (notably in the United Kingdom and Sweden) require some form of analysis or measures to reduce the potential for progressive collapse. However, there is no specific engineering design method prescribed for the structural design process to prevent progressive collapse. Unless a building is being designed to meet the GSA or DoD criteria, it is up to the owner and the design team to decide how much progressive collapse analysis and mitigation to incorporate into their design.

To address blast resistance (Chapter 4 contains a detailed discussion of explosive blast theory) and to minimize the possibility of progressive collapse, the priority of upgrades should be based on the relative importance of a structural or non-structural element, in the order below:

- **Primary structural elements.** These are the essential parts of the building's resistance to catastrophic blast loads and

progressive collapse (e.g., columns, girders, roof beams, and the main lateral resistance system).

- **Secondary structural elements.** These include all other load bearing members (e.g., floor beams, slabs, etc.).
- **Primary non-structural elements.** These are the elements (including their attachments) that are essential for life safety systems or elements that can cause substantial injury if failure occurs (e.g., ceilings or heavy suspended mechanical units).
- **Secondary non-structural elements.** These include elements not covered in primary non-structural elements (e.g., partitions, furniture, and light fixtures).

Priority should be given to the critical elements that are essential to mitigating the extent of collapse. Designs for secondary structural elements should minimize injury and damage. Consideration should be given to reducing damage and injury from primary as well as secondary non-structural elements. For example, if an explosive event causes the local failure of one column, which results in major collapse within a structural bay, a design that mitigated progressive collapse would preclude the additional loss of primary structural members beyond this localized damage zone (i.e., the loss of additional columns, main girders, etc.). This would not necessarily preclude the additional loss of secondary structural or non-structural elements outside the initial zone of localized damage, provided the loss of such members is acceptable for that performance level and the loss does not precipitate the onset of progressive collapse.

### 3.2.3 Loads and Stresses

Structures should be designed to resist blast loads. The DoD designates the level of blast protection a building must meet based on how many occupants it contains and its function. The demands on the structure will be equal to the combined effects of dead, live, and blast loads. Blast loads or dynamic rebound may occur in directions opposed to typical gravity loads.

For purposes of designing against progressive collapse, loads should be defined as dead load plus a realistic estimate of actual live load. The value of the live load may be as low as 25 percent of the code-prescribed live load. The design should use ultimate strengths with dynamic enhancements based on strain rates. Allowable responses are generally post elastic.

### 3.2.4 Good Engineering Practice Guidelines

The following guidelines are commonly used to mitigate the effects of blast on structures and to mitigate the potential for progressive collapse. Details and more complete guidance are available in the references below. These guidelines are not meant to be complete, but are provided to assist the designer in the initial evaluation and selection of design approaches. For higher levels of protection from blast, cast-in-place reinforced concrete is normally the construction type of choice. Other types of construction such as properly designed and detailed steel structures are also allowed. Several material and construction types, although not disallowed by these criteria, may be undesirable and uneconomical for protection from blast.

#### The following additional references are recommended:

- **Biggs, John M.** *Introduction to Structural Dynamics*. McGraw-Hill. (1964).
- **The Institute of Structural Engineers.** *The Structural Engineer's Response to Explosive Damage*. SETO, Ltd., 11 Upper Belgrave Street, London SW1X8BH. (1995).
- **Mays, G.S. and Smith, P.D.** *Blast Effects on Buildings: Design of Buildings to Optimize Resistance to Blast Loading*. Thomas Telford Publications, 1 Heron Quay, London E14 4JD. (1995).
- **National Research Council.** *Protecting Buildings from Bomb Damage*. National Academy Press. (1995).
- Consider incorporating internal damping into the structural system to absorb the blast impact.
- The use of symmetric reinforcement can increase the ultimate load capacity of the structure.
- Consider wire mesh in plaster to reduce the incidence of flying fragments.
- Avoid the use of masonry when blast is a threat. Masonry walls break up readily and become secondary fragments during blasts.

- The use of multiple barrier materials and construction techniques can sometimes accomplish the same goal with less expense than a single material or technique.
- The designer should recognize that components might act in directions for which they were not designed. This is due to the engulfment of structural members by blast, the negative phase, the upward loading of elements, and dynamic rebound of members. Making steel reinforcement (positive and negative faces) symmetric in all floor slabs, roof slabs, walls, beams, and girders will address this issue. Symmetric reinforcement also increases the ultimate load capacity of the members.
- Lap splices should fully develop the capacity of the reinforcement.
- Lap splices and other discontinuities should be staggered.
- Deflections around certain members, such as windows, should be controlled to prevent premature failure. Additional reinforcement is generally required.
- In general, column spacing should be minimized so that reasonably sized members can be designed to resist the design loads and increase the redundancy of the system. A practical upper level for column spacing is 30 feet for the levels of blast loads described herein.
- In general, floor to floor heights should be minimized. Unless there is an overriding architectural requirement, a practical limit is generally less than or equal to 16 feet.
- It is recommended that the designer use fully grouted and reinforced concrete masonry unit (CMU) construction when CMU is selected.
- It is essential that the designer actively coordinate structural requirements for blast with other disciplines, including architectural and mechanical.

- The use of one-way wall elements spanning from floor-to-floor is generally a preferred method to minimize blast loads imparted to columns.
- In many cases, the ductile detailing requirements for seismic design and the alternate load paths provided by progressive collapse design assist in the protection from blast. The designer must bear in mind, however, that the design approaches are, at times, in conflict. These conflicts must be worked out on a case by case basis.
- It is recommended that architectural or structural features be used that deny contact with exposed primary vertical load members. A minimum stand-off of at least 6 inches from these members is required.

### **3.2.5 Building Materials**

All building materials and types acceptable under model building codes are allowed; however, special consideration should be given to materials that have inherent flexibility and that are better able to respond to load reversals (i.e., cast in place reinforced concrete and steel construction). Careful detailing is required for material such as pre-stressed concrete, pre-cast concrete, and masonry (brick and concrete masonry unit) to adequately respond to the design loads. The construction type selected must meet all performance criteria of the specified level of protection.

### **3.2.6 Methods and References**

All building components requiring blast resistance should be designed using established methods and approaches for determining dynamic loads, structural detailing, and dynamic structural response. Design and analysis approaches should be consistent with those in the technical manuals or the GSA *Security Design Criteria* and the American Society of Civil Engineers *Minimum Design Loads for Buildings and Other Structures*, ASCE 7. Alternative analysis and mitigation methods are permitted, provided that the performance level is attained. A peer group should evaluate new and untested methods.

## **3.3 BUILDING ENVELOPE**

### **3.3.1 Building Exterior**

At the building exterior, the focus shifts from deterring and delaying the attack, to mitigating the effects of an explosion. The exterior envelope of the building is the most vulnerable to an exterior explosive threat because it is the part of the building closest to the weapon.

It also is a critical line of defense for protecting the occupants of the building from CBR threats. Significant quantities of air can enter a building by means of infiltration through unintentional leakage paths in the building envelope. Such leakage is of more concern during an exterior CBR release, such as a large-scale attack, than for a directed terrorist act. The reduction of air leakage is a matter of tight building construction in combination with building pressurization. Although building pressurization may be a valuable CBR-protection strategy in any building, it is much more likely to be effective in a tight building. However, to be effective, filtration of building supply air must be appropriate for the CBR agent introduced. Although increasing the air tightness of an existing building can be more challenging than during new construction, it should still be seriously considered.

The design philosophy to be used here is that simpler is better. Generally, simple geometries, with minimal ornamentation (which may become flying debris during an explosion) are recommended. If ornamentation is used, it is recommended that it consist of lightweight material such as timber or plastic, which is less likely to become a projectile in the event of an explosion than, for example, brick, stone, or metal.

Soil can be highly effective in reducing the impact of a major explosive attack. Bermed walls and buried rooftops have been found to be highly effective for military applications and can be effectively extended to conventional construction. This type of solution can also be effective in improving the energy efficiency of the

building. Note that, if this approach is taken, no parking should be permitted on top of the building.

### **3.3.2 Exterior Wall Design**

The exterior walls provide the first line of defense to prevent air-blast pressures and hazardous debris from entering the building. They would be subject to direct reflected pressures from an explosive threat located directly across from the wall along the secured perimeter line. If the building is more than four stories high, it may be advantageous to consider the reduction in pressure with height due to the increased distance and angle of incidence. At a minimum, the objective of design is to ensure that these members fail in a flexible mode rather than a brittle mode such as shear. The walls also need to be able to resist the loads transmitted by the windows and doors. It is not uncommon for bullet-resistant windows to have a higher ultimate capacity than the walls to which they are attached. Beyond ensuring a flexible failure mode, the exterior wall may be designed to resist the actual or reduced pressure levels of the defined threat. Special reinforcing and anchors should be provided around blast-resistant window and door frames.

Poured-in-place reinforced concrete will provide the highest level of protection, but solutions like pre-cast concrete, reinforced CMU block, and metal studs may also be used to achieve lower levels of protection.

For pre-cast panels, consider a minimum thickness of 5 inches with two-way reinforcing bars spaced not greater than the thickness of the panel. Connections into the structure should provide a straight line of load transmittal, using as few connecting pieces as possible.

For CMU block walls, use 8-inch block walls, fully grouted with vertical centered reinforcing bars placed in each cell and horizontal reinforcement at each layer. Connections into the structure should be able to resist the ultimate lateral capacity of the wall. A preferred system is to have a continuous exterior CMU wall that laterally bears against the floor system. For increased protection, consider using 12-inch blocks with two layers of reinforcement.



For metal stud systems, use metal studs back to back and mechanically attached, to minimize lateral torsion effects. To catch exterior cladding fragments, attach a wire mesh to the exterior side of the metal stud system. The supports of the wall are to be designed to resist the ultimate lateral capacity load of the system.

**Exterior Walls.** For the design of exterior walls, consider the following:

- Exterior walls should resist the actual pressures and impulses acting on the exterior wall surfaces from the threats defined for the facility.
- Exterior walls should be capable of withstanding the dynamic reactions from the windows.
- Shear walls that are essential to the lateral and vertical load bearing system, and that also function as exterior walls, should be considered primary structures. Design exterior shear walls to resist the actual blast loads predicted from the threats specified.
- Special consideration should be given to construction types that reduce the potential for collapse where exterior walls are not designed for the full design loads.
- By U.S. military standards (per Army Technical Manual 5-853), a medium protection level for walls would be the equivalent of 4-inch concrete with #5 reinforcing steel at 6-inch intervals each way or 8-inch CMU with #4 reinforcing steel at 8-inch intervals. TM 5-853 provides other alternatives for low, medium, and high protection.

**Cladding and Finishes.** Designers should consider the following:

- Substitute strengthened building elements and systems when stand-off distances cannot be accommodated.
- Use ductile materials capable of very large plastic deformations without complete failure.
- Provide blast-resistant walls when a high threat is present.

- Consider use of sacrificial exterior wall panels to absorb blast.
- Use earthtone-colored materials and finishes on exterior surfaces to diminish the prominence of a building.
- Consider reinforced concrete wall systems in lieu of masonry or curtain walls to minimize flying debris in a blast.
- Reinforced wall panels can protect columns and assist in preventing progressive collapse, because the wall will assist in carrying the load of a damaged column.

**Exterior Column Design.** Exterior columns should be designed to resist the peak reflected pressure of an explosive event, including the load transmitted by supported walls. Because these elements are slender, the air-blast tends to “wash around” them if they are free standing, reducing the duration of the loading. This is referred to as a “clearing time” effect. Although it is conservative to neglect these effects, it may be advantageous to take them into account in some situations, like close-in explosions. The design must provide for both the axial and flexible loads and stability. For concrete columns, spiral reinforcing or closed stirrups should be placed at a spacing of not less than half the minimum thickness of the member to ensure that adequate confinement and ductility are provided. For steel columns, the connections are the most vulnerable part of the design. If possible, place the base plate below ground level and protect with concrete and use multi-story segments for the lower floors.

### **3.3.3 Window Design**

Window systems on the exterior façade of a building should be designed to mitigate the hazardous effects of flying glass during an explosion event. Designs should integrate the features of the glass, connection of the glass to the frame (bite), and anchoring of the frame to the building structure to achieve a “balanced design.” This means all the components should have compatible capacities and theoretically would all fail at the same pressure-pulse levels. In this way, the damage sequence and extent of damage are controlled. Table 3-1 presents six GSA glazing protection levels based

on how far glass fragments would enter a space and potentially injure its occupants. Figure 3-4 depicts how far glass fragments could enter a structure for each GSA performance condition.

The divide between performance conditions 3a and 3b can be equated to the “threshold of injury.” The divide between performance conditions 4 and 5 can be equated to the “threshold of lethality.” The GSA glazing performance conditions shown below correlate with the DoD levels of protection presented in Table 3-2.

**Glass Design.** Four types of glass are commonly used in window glazing systems: annealed glass, heat strengthened glass, fully thermally tempered glass, and polycarbonate. Other types of glass materials exist, but are not commonly used in typical commercial window systems. Of the four common types, annealed glass and fully thermally tempered glass are the type of windows for most of-fice buildings.

Table 3-1: Glazing Protection Levels Based on Fragment Impact Locations<sup>1</sup>

Performance Condition	Protection Level	Hazard Level	Description of Window Glazing Response
1	Safe	None	Glazing does not break. No visible damage to glazing or frame.
2*	Very High	None	Glazing cracks, but is retained by the frame. Dusting or very small fragments near sill or on floor acceptable.
3a*	High	Very Low	Glazing cracks. Fragments enter space and land on floor no more than 3.3 feet from the window.
3b*	High	Low	Glazing cracks. Fragments enter space and land on floor no more than 10 feet from the window.
4*	Medium	Medium	Glazing cracks. Fragments enter space and land on floor and impact a vertical witness panel at a distance of no more than 10 feet from the window at a height no greater than 2 feet above the floor.
5*	Low	High	Glazing cracks and window system fails catastrophically. Fragments enter space, impacting a vertical witness panel at a distance of no more than 10 feet from the window at a height greater than 2 feet above the floor.

\* In conditions 2, 3a, 3b, 4 and 5, glazing fragments may be thrown to the outside of the protected space toward the detonation location.

<sup>1</sup> From GSA PBS-PQ100.1, *Facilities Standards for the Public Building Service*, June 14, 1996

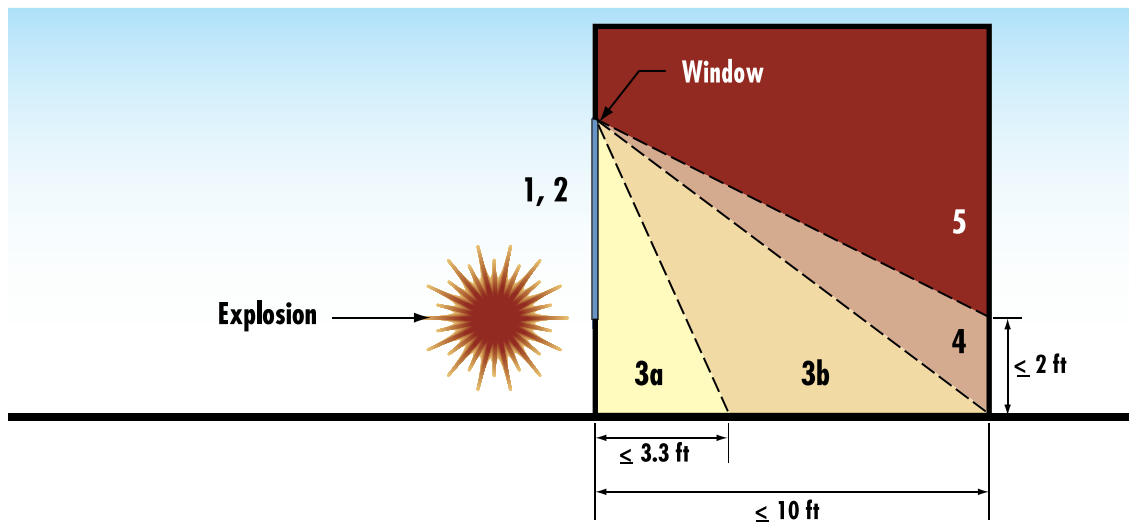


Figure 3-4 Side view of a test structure illustrating performance conditions of Table 3-2

Table 3-2:  
Correlation of GSA Glazing Performance Conditions and DoD Levels of Protection for New Buildings

GSA Glazing Performance Condition	Corresponding DoD Level of Protection for New Buildings
1	High
2	Medium
3a	Low
3b/4	Very Low
5	Below antiterrorism (AT) Standards

Annealed glass, also known as float, plate, or sheet glass, is the most common glass type used in commercial construction. Annealed glass is of relatively low strength and upon failure, fractures into razor sharp, dagger-shaped fragments (see Figure 3-5).

Fully thermally tempered glass (TTG) is typically four to five times stronger than annealed glass with a design stress of 16,000 psi (112,000 kPa). The fracture characteristics of tempered glass are superior to those of annealed glass. Upon failure, it will eventu-

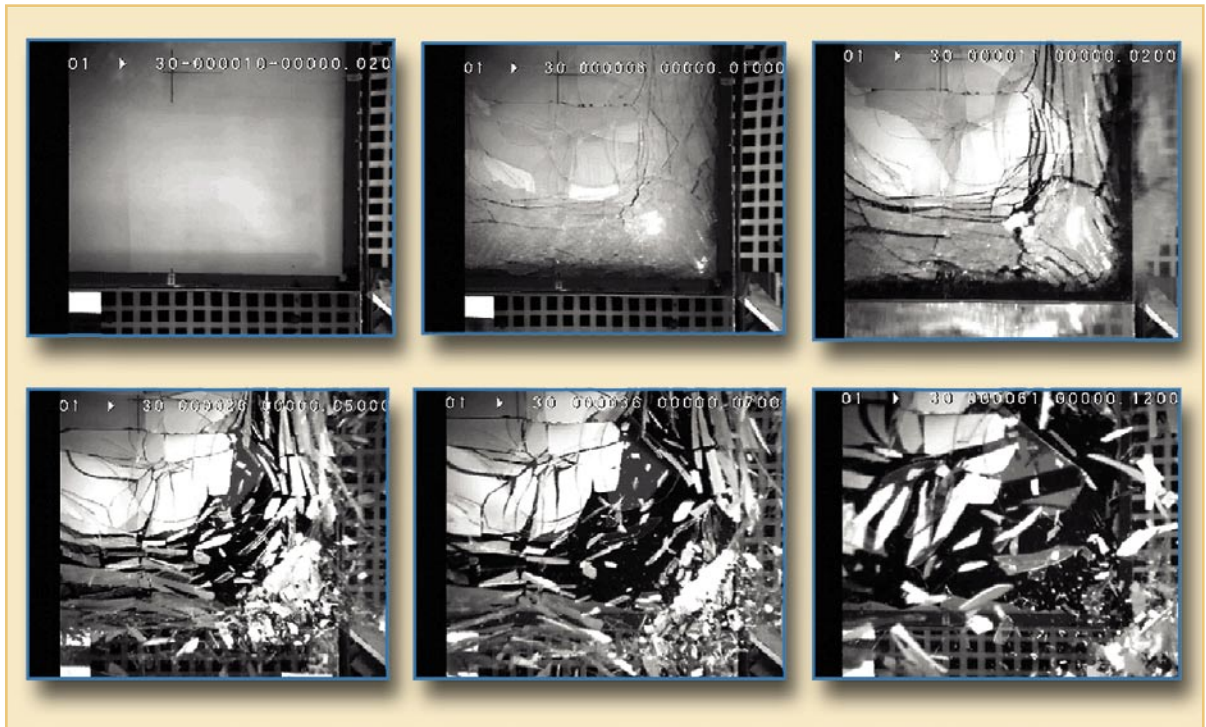


Figure 3-5 An unprotected window subject to a large explosion

ally fracture into small cube-shaped fragments. Breakage patterns of side and rear windows in American automobiles are a good example of the failure mode of thermally tempered glass. Current building codes generally require thermally tempered glass anywhere the public can physically touch the glass such as entrance doors and sidelights. Although thermally tempered glass exhibits a relatively safe failure mode for conventional usage, failure under blast loading still presents a significant health hazard. Results from blast tests reveal that, upon fracture, TTG fragments may be propelled into cohesive clumps that only fragment upon impact into smaller rock salt-type fragments. Even if the tempered glass breaks up initially into small fragments, the blast overpressure can propel the fragments at a high enough velocity to constitute a severe hazard.

Wire-reinforced glass is a common glazing material. It consists of annealed glass with an embedded layer of wire mesh. Its primary use is as a fire-resistant and forced entry barrier. Wire-reinforced glass has the fracture and low strength characteristics of annealed

glass and, although the wire binds some fragments, it still ejects a considerable amount of sharp glass and metal fragments. Wire-reinforced glass is not recommended for blast-resistant windows.

Laminated glass is a pane with multiple glass layers and a pliable interlayer material (usually made from polyvinyl butyral (PVB)) between the glass layers. Combining interlayer bonding materials with layers of glass produces cross-sections that perform well against blast, ballistic, and forced entry attacks. The interlayer acts as the glue that bonds the multiple layers of glass into a single pane of a given thickness and provides a membrane response after the glass layers crack under loading. Laminated glass offers significant advantages over monolithic glass. It is stronger and, if failure occurs, the interlayer material may retain most of the glass fragments. Also, if a projectile passes through the glass, most spalling glass fragments will be retained. Increased safety for fragment retention can be obtained in the event of catastrophic failure from an explosive blast by placing a decorative crossbar or grillwork on the interior of the glazing. Note, crossbars must be mounted across the center of mass of each window pane to be effective.

Another treatment used for mitigating the effects of an explosive attack is security window film. The polyester film used in commercial products is commonly referred to as fragment retention film (FRF), safety film, security film, protective film, or shatter-resistant film. These films are adhered to the interior surface of the window to provide fragment retention and reduce the overall velocity of the glass fragments at failure. Fragment retention film combines a strong pressure sensitive adhesive with a tough polyester layer. Four methods are used to attach security film to windows: a daylight attachment (applied only to the vision opening); edge-to-edge attachment (applied out to the edge of the glass); wet-glazed attachment (daylight or edge-to-edge film with a silicone bead along edge of the frame); and a mechanical attachment. Because fragment retention film applies directly to the glass surface of a window pane, it is beneficial for retrofitting existing windows as well as on new windows.

Fragment retention film behaves similarly to relatively thin laminated and polycarbonate glazing in terms of fragmentation. It is available in common thicknesses of 2, 4, 7, and 10 mils. Fragment retention film improves the performance of the glass under blast loading to varying degrees, depending on the thickness, quality, and type of film installation. The best performance is achieved when the film is installed into the bite of the glazing or is connected to the frame. Fragment retention film can also provide solar control benefits. As with laminates, increased safety can be obtained with window films by placing a decorative crossbar or grillwork on the interior of the glazing.

Thermoplastic polycarbonates are very strong and suitable for blast- and forced entry-resistant window design. Monolithic polycarbonate is available in thicknesses up to ½ inch, but can be fused together to obtain any thickness needed. However, polycarbonate is expensive and subject to environmental degradation (especially from exposure to aromatic hydrocarbons) and abrasion. Local building codes should be consulted when considering polycarbonates. There are several fire safety issues associated with its use (thermoplastic polycarbonate is rated as a class CC-1 material and will often test with a smoke density rating over 500). Additionally, because of its strength, local fire codes may require a percentage of polycarbonate glazing to pop out for emergency egress.

**Frame and Anchorage Design.** Window frames need to retain the glass so that the entire pane does not fall out and also should be designed to resist the breaking stress of the window glass. To retain the glass in the frame, a minimum of a ¼-inch bead of structural sealant (i.e., silicone or polyvinyl butyral) should be used around the inner perimeter of the window. The allowable tensile strength should be at least 20 psi. Also, the window bite (i.e., the depth of window captured by the frame) needs to be at least ½ inch. In some applications (e.g., the lobby area where large panes of glass are used), a larger bite with more structural sealant may be needed. Frame and anchorage design is performed by applying the breaking strength of the window to the frame and the fasteners. In most conventionally designed

buildings, the frames will be aluminum; however, in some applications, steel frames are used.

**Mullion and Wall Design.** The frame members connecting adjoining windows are referred to as mullions. These members may be designed using a static approach when the breaking strength of the window glass is applied to the mullion, or a dynamic load may be applied using the peak pressure and impulse values. Although the static approach may seem easier, it often yields a design that is not practical, because the mullion can become very deep and heavy, driving up the weight and cost of the window system. In addition, it may not be consistent with the overall architectural objectives of the project. A dynamic approach is likely to provide a section that meets the design constraints of the project. To accomplish this, a single-degree-of-freedom solution is often used. The governing equation of motion may be solved using numerical methods. There are also charts available for linearly decaying loads that circumvent the need to solve differential equations. These charts only require that the fundamental period of the mullion (including the tributary area of the window glass), the ultimate resistance force of the mullion, the peak pressure, and the equivalent linear decay time are known.

Peak lateral response of the mullion is to be limited to a 2-degree support rotation. Also, the displacement ductility is to be limited to a 4-degree support rotation. As with frames, it is good engineering practice to limit the number of interlocking parts used for the mullion.

A similar approach may be used for checking the response of the supporting wall response. It makes no sense to have blast mitigating windows if they are stronger than the wall that they are anchored into. The maximum strength of any window and anchorage system should be equal to the wall strength. This becomes particularly important in the design of ballistic-resistant and forced entry mitigating windows, which consist of one or more inches of glass and polycarbonate. These windows can easily become stronger than the supporting wall. In some applications, even the use of tempered glass can become problematic.



**Design up to Specified Load.** Window systems design (glazing, frames, anchorage to supporting walls, etc.) on the exterior facade should be balanced to mitigate the hazardous effects of flying debris in an explosive event. The walls, anchorage, and window framing should fully develop the capacity of the glazing material selected. The designer may use a combination of methods such as government produced and sponsored computer programs (e.g., Window Lite Analysis Code (WINLAC), Safety Viewport Analysis Code (SAFEVU), Blast-Resistant Window Program (BLASTOP), and Window Glazing Analysis Response and Design (WINGARD)) coupled with test data and recognized dynamic structural analysis techniques to show that the glazing either survives the specified threats or the post damage performance of the glazing protects the occupants in accordance with the conditions specified in Table 3-2. In general, laminated glass is the preferred glazing material for new construction. Tests have shown that laminated glass performs well under blast loads if mounted in properly designed window frames and it can be engineered to offer the highest levels of protection from glass fragments.

**Limitation of Glass Hazard Mitigation.** Keep in mind that the pressures exerted on a building in a large explosion (e.g., a truck bomb) are often significantly greater than the pressures for which protected windows are designed. For these large events, the upgraded solutions may not be effective, except for windows on the sides of the building not facing the explosion or adjacent buildings. This is particularly true if structural damage occurs. Flying debris generated by structural damage typically causes more severe injuries than window damage alone; however, blast mitigating window designs are expected to be effective for a large number of threats where the pressures are low. Two such scenarios include a package bomb near the building and a truck bomb that goes off a block away.

Although these solutions do provide protection at modest pressure levels, they are not a “magic shield.” The threat of attack still exists and injuries may still occur if an attack occurs. These measures will be most effective if considered a “last resort” measure

used in conjunction with a full range of physical and operational security measures at the facility.

**General Guidelines for Windows and Glazing.** General guidelines for windows and glazing include the following:

- Do not place windows adjacent to doors because, if the windows are broken, the doors can be unlocked.
- Minimize the number and size of windows in a facade. If possible, limit the amount of glazed area in building facades to 15 percent. The amount of blast entering a space is directly proportional to the amount of openings on the facade.
- Consider using burglary- and ballistic-resistant glazing in high-risk buildings.
- Consider using laminated glass in place of conventional glass.
- Consider window safety laminate (such as mylar) or another fragment retention film over glazing (properly installed) to reduce fragmentation.
- Consider placing guards, such as grills, screens, or meshwork, across window openings to protect against covert entry. Affix protective window guards firmly to the structure.
- Consider installing blast curtains, blast shades, or spall shields to prevent glass fragments from flying into the occupied space.
- Consider curtains, blinds, and shades to limit entry of incendiary devices.
- Consider narrow recessed windows with sloped sills because they are less vulnerable than conventional windows (see Figure 3-6).
- Consider windows with key-operated locks because they provide a greater level of protection than windows with simple latches. Stationary, non-operating windows are preferred for security.
- Position the operable section of a sliding window on the inside of the fixed section and secure it with a broomstick, metal rod, or similar device placed at the bottom of the track.



Figure 3-6 Narrow and recessed windows with sloped sills

SOURCE: U.S. AIR FORCE, *INSTALLATION FORCE PROTECTION GUIDE*

- Provide horizontal windows 6 feet above the finished floor to limit entry.
- Harden the windows by using steel window frames securely fastened or cement grouted to the surrounding structure.

**Additional Glazing Requirements.** Additional glazing requirements include the following:

- Ballistic windows, if required, should meet the requirements of Underwriters Laboratory (UL) 752 Bullet-Resistant Glazing for a level appropriate for the project. Glassclad polycarbonate or laminated polycarbonate are two types of acceptable glazing material.
- Security glazing, if required, should meet the requirements of the American Society for Testing and Materials (ASTM) F1233 or UL 972, Burglary-Resistant Glazing Material.
- Glazing should meet the minimum performance specified in Table 3-2; however, special consideration should be given to frames and anchorages for ballistic-resistant windows and security glazing because their inherent resistance to blast may impart large reaction.

- Resistance of window assemblies to forced entry (excluding glazing) should meet the requirements of ASTM F 588 for a grade appropriate for the project.
- Interior glazing should be minimized where a threat exists. The designer should avoid locating critical functions next to high-risk areas with glazing, such as lobbies, loading docks, etc.

**Multi-hazard Considerations.** Under normal operating conditions, windows function in a variety of ways, including:

- Allowing light into a building
- Conserving energy by reducing thermal transmission
- Reducing noise through acoustic transmission

Explosions are one of a number of abnormal loading conditions that the building may be designed to mitigate. Some of the others are fire, earthquake, hurricane, gunfire, and forced entry.

In developing a protection strategy for windows to mitigate the effects of a particular explosion threat scenario, it is important to consider how this protection may interfere with some of these other functions or other explosion threat scenarios. Some questions that may be worthwhile to consider are:

- If an internal explosion occurs, will the upgraded windows increase smoke inhalation injuries by preventing the smoke from venting through windows that would normally break in an explosion event?
- If a fire occurs, will it be more difficult to break protected windows in order to vent the building and gain access to the injured?
- Will a window upgrade that is intended to protect the occupants worsen the hazards to passersby?

### 3.3.4 Doors

A door system includes the door, frame, and anchorage to the building. As part of a balanced design approach, exterior doors in high-risk buildings should be designed to withstand the maximum dynamic pressure and duration of the load from the design threat explosive blast. Other general door considerations are as follows:

- Provide hollow steel doors or steel-clad doors with steel frames.
- Provide blast-resistant doors for high threats and high levels of protection.
- Limit normal entry/egress through one door, if possible.
- Keep exterior doors to a minimum while accommodating emergency egress. Doors are less attack-resistant than adjacent walls because of functional requirements, construction, and method of attachment.
- Ensure that exterior doors open outward from inhabited areas. In addition to facilitating egress, the doors can be seated into the door frames so that they will not enter the buildings as hazardous debris in an explosion.
- Replace externally mounted locks and hasps with internally locking devices because the weakest part of a door system is the latching component.
- Install doors, where practical, so that they present a blank, flush surface to the outside to reduce their vulnerability to attack.
- Locate hinges on the interior or provide concealed hinges to reduce their vulnerability to tampering.
- Install emergency exit doors so that they facilitate only exiting movement.
- Equip any outward-opening double door with protective hinges and key-operated mortise-type locks.
- Provide solid doors or walls as a backup for glass doors in foyers.
- Strengthen and harden the upright surfaces of door jambs.

### 3.3.5 Roof System Design

For an explosive threat, the primary loading on the roof is downward over-pressure. Secondary loads include upward pressure due to the blast penetrating through openings and upward suction during the negative loading phase. The upward pressures may have an increased duration due to multiple reflections of the air-blast internally. It is conservative to consider the downward and upward loads separately.

The preferred system is to use poured-in-place reinforced concrete with beams in two directions. If this system is used, beams should have stirrups along the entire span spaced not greater than one half the beam depths. A second system uses steel frames with a concrete and metal deck slab to achieve higher levels of protection. For this system to work well, a two-way system of reinforcing bars spaced not more than the total thickness of the slab should be provided. Also, puddle welds or other robust systems are needed along the perimeter to resist the shear forces on the slab as it deflects downward.

Less desirable systems include metal plate systems without concrete, and precast and pre/post tensioned systems. The metal plate system is prone to fail due to its light weight and direct pressure, or by the negative phase pressure that creates a suction effect on the roof. Precast panels are problematic because of the tendency to fail at the connections. Pre/post tensioned systems tend to fail in a brittle manner if stressed beyond their elastic limit and they also are not able to accept upward loads without additional reinforcement. If pre/post tensioned systems are used, continuous mild steel needs to be added to the top and the bottom faces to provide the flexibility needed to resist explosion loads.

Flat slab/plate systems are also less desirable because of limited two-way action and the potential of shear failure at the columns.

**Miscellaneous Roof System.** Designers should consider the following:

- Designing buildings with a sacrificial sloping roof that is above a protected ceiling (see Figure 3-7).

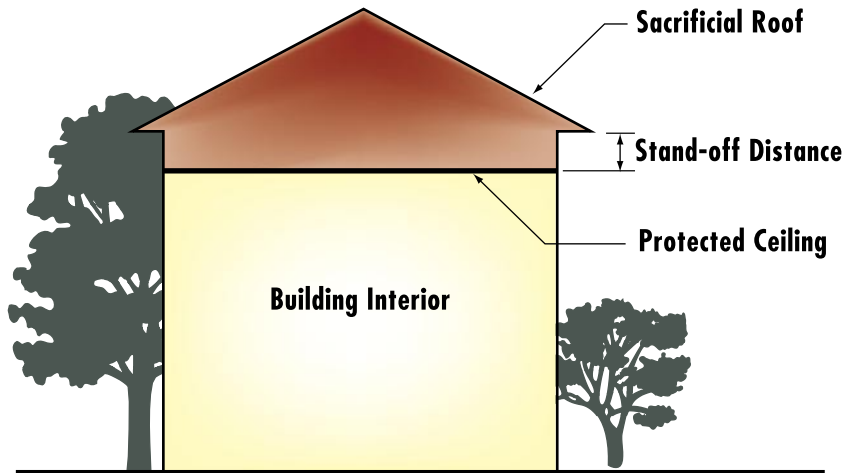


Figure 3-7 Sacrificial roof

- Controlling access to roofs to minimize the possibility of aggressors placing explosives or chemical, biological, or radiological agents there or otherwise threatening building occupants or critical infrastructure. For new buildings, eliminate all external roof access by providing access from internal stairways or ladders, such as in mechanical rooms. For existing buildings, eliminate external access where possible or make roof access ladders removable, retractable, or lockable.
- Protecting roof openings to a facility from covert entry by installing screens or grates or attaching Intrusion Detection System sensors.

### 3.4 MECHANICAL SYSTEMS

Mechanical system design standards address limiting damage to critical infrastructure and protecting building occupants against CBR threats. The primary goal of a mechanical system after a terrorist attack should be to continue to operate key life safety systems. This can be accomplished by locating components in less vulnerable areas, limiting access to mechanical systems, and providing a reasonable amount of redundancy. Other aspects of mechanical systems are discussed in Section 2.10.

During an interior bombing event, smoke removal and control are of paramount importance. The designer should consider the fact that, if window glazing is hardened, a blast may not blow out windows, and smoke may be trapped in the building. In the event of a blast, the available smoke removal system may be essential to smoke removal, particularly in large, open spaces. This equipment should be located away from high-risk areas (e.g., garages and loading docks). The system controls and power wiring to the equipment should be protected, and the system should be connected to emergency power to provide smoke removal. Smoke removal equipment should be provided with standalone local control panels that can continue to individually function in the event the control wiring is severed from the main control system.

Designers should consider the following:

- Do not mount plumbing, electrical fixtures, or utility lines on the inside of exterior walls, but, when this is unavoidable, mount fixtures on a separate wall at least 6 inches from the exterior wall face.
- Avoid placing plumbing on the roof slab.
- Avoid suspending plumbing fixtures and piping from the ceiling.
- Reduce the number of utility openings, manholes, tunnels, air conditioning ducts, filters, and access panels into the structure.
- Locate utility systems away from likely areas of potential attack, such as loading docks, lobbies, and parking areas.
- Protect building operational control areas and utility feeds to lessen the negative effects of a blast.
- Design operational redundancies to survive all kinds of attack.
- Use lockable systems for utility openings and manholes where appropriate. Infrequently used utility covers/manholes can be tack-welded as an inexpensive alternative to locking tamper-resistant covers.



**Key HVAC System Considerations.** The following HVAC design measures (from Centers for Disease Control and Prevention, National Institute for Occupational Safety and Health, *Guidance for Protecting Building Environments from Airborne Chemical, Biological, or Radiological Attacks*, May 2002) should be considered to mitigate the risk of CBR threats for high security buildings. HVAC protective actions are discussed in Chapter 5.

- Elevating the fresh-air intakes to reduce the potential for hazardous materials entering a building from a ground-level outdoor release is most easily applied in new construction (see Figures 3-8 and 3-9). This has two main benefits. The first benefit is that it provides passive security against malicious acts, which makes it more difficult for a container of hazardous material to be inserted directly into the building's HVAC system and to be conveyed to various parts of the building. The second benefit is that it makes it less likely that high concentrations of hazardous material will occur at the intakes if there is a ground-level release near the building.
- Locating ground-level intakes near streets or parking areas can cause exhaust fumes to be drawn indoors under certain conditions of wind and stability (see Figure 3-10). In elevating the intakes, the dilution increases with the distance from the source. In stable conditions, contaminants released near the ground will likely remain close to the ground unless the airflow over the building lifts it upward. Contaminants that are heavier than air will also tend to remain close to the ground under calm conditions.
- Placing intakes at the highest practical level on the building is beneficial. For protection against malicious acts, the intakes should also be covered by screens so that objects cannot be tossed into the intakes or into air wells from the ground (see Figure 3-10). Such screens should be sloped to allow thrown objects to roll or slide off the screen, away from the intake. Many existing buildings have air intakes that are located at or below ground level. For those that have wall-mounted or below-grade intakes close to the building, the intakes can be elevated

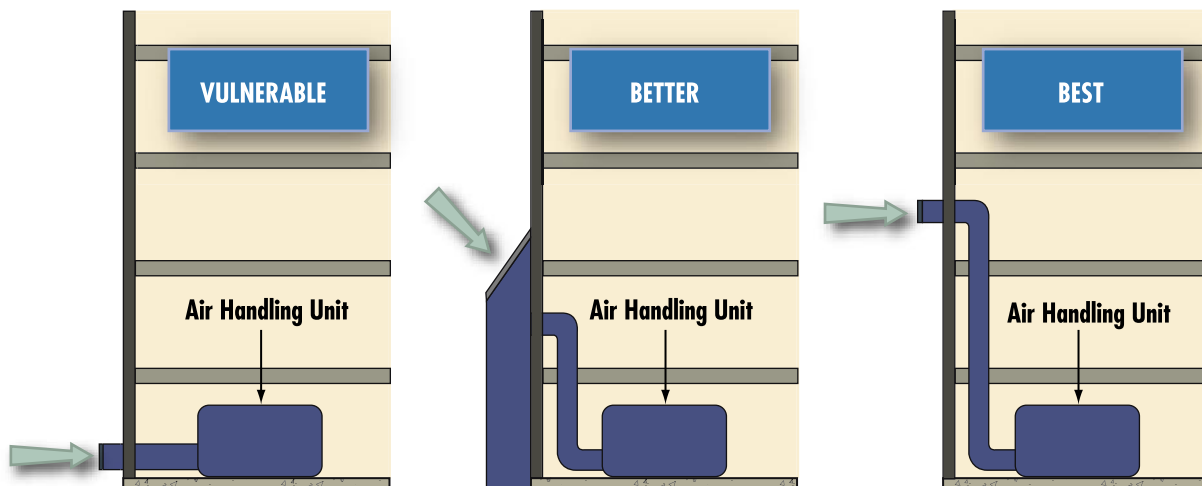
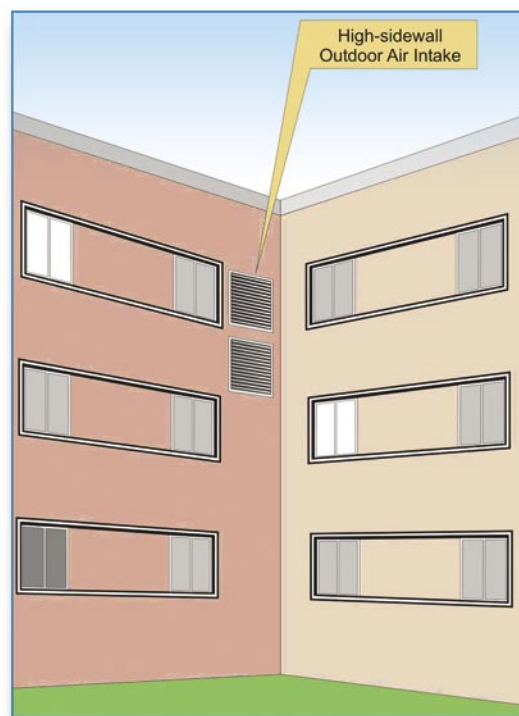


Figure 3-8 Example of protecting outdoor air intakes

SOURCE: CDC/NIOSH, PUBLICATION NO. 2002-139, *GUIDANCE FOR PROTECTING BUILDING ENVIRONMENTS FROM AIRBORNE CHEMICAL, BIOLOGICAL, OR RADIOLOGICAL ATTACKS*, MAY 2002

Figure 3-9  
Example of elevated air intake



SOURCE: CDC/NIOSH, PUBLICATION NO. 2002-139, *GUIDANCE FOR PROTECTING BUILDING ENVIRONMENTS FROM AIRBORNE CHEMICAL, BIOLOGICAL, OR RADIOLOGICAL ATTACKS*, MAY 2002

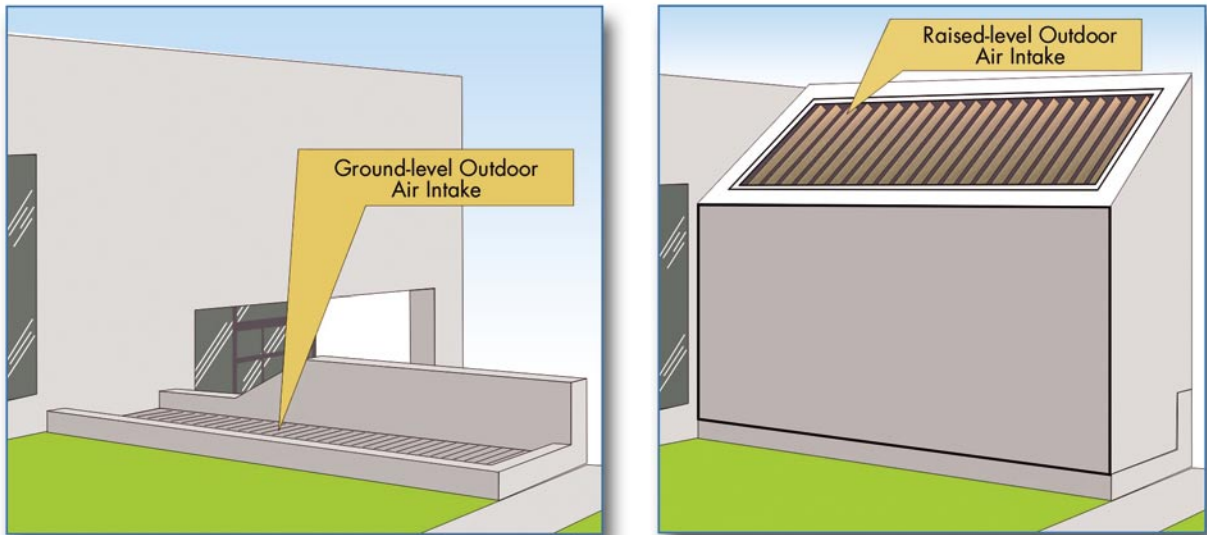


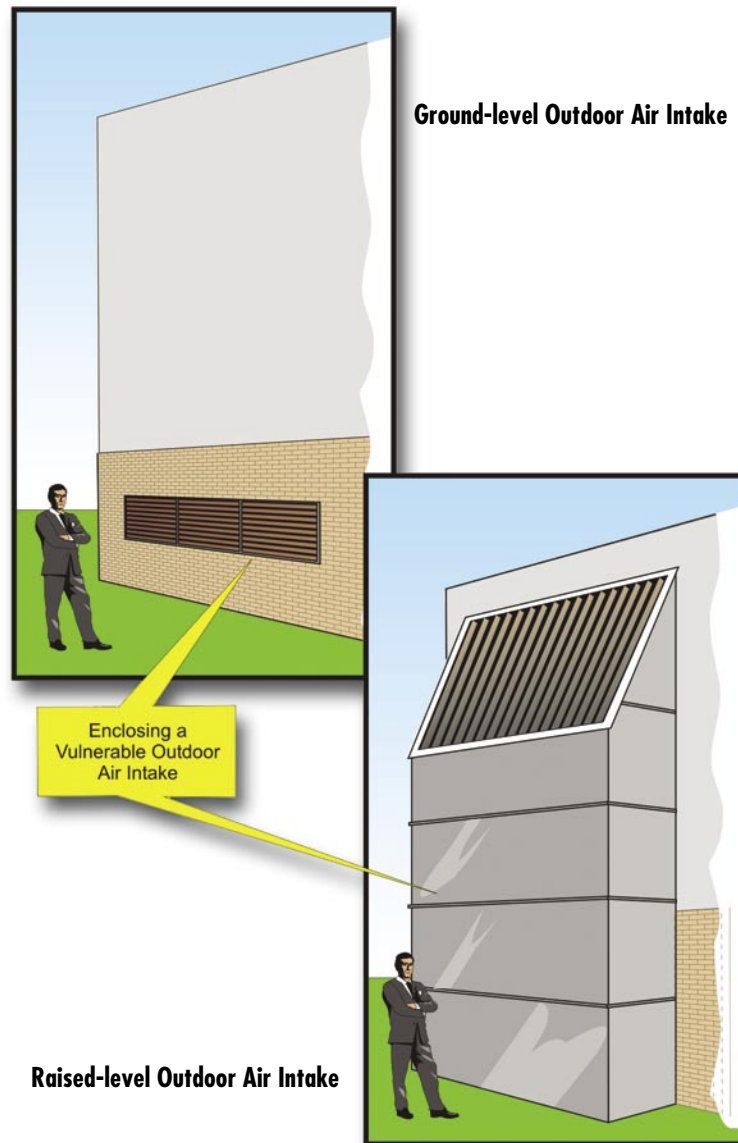
Figure 3-10 Another example of protecting outdoor air intakes

SOURCE: CDC/NIOSH, PUBLICATION NO. 2002-139, *GUIDANCE FOR PROTECTING BUILDING ENVIRONMENTS FROM AIRBORNE CHEMICAL, BIOLOGICAL, OR RADIOLOGICAL ATTACKS*, MAY 2002

by constructing a plenum or external shaft over the intake (see Figure 3-11). An extension height of 12 feet will place the intake out of reach of individuals without some assistance.

- Effectively elevating intakes has practical limits. A plume or cloud of hazardous materials can reach the intakes, particularly if the source is large and distant. For low-rise buildings (i.e., those having a width more than twice the height), a plume originating at ground level near the building will travel over the building rather than around it; thus, the wind will convey contaminants to the top of the building, with some dilution occurring.
- For existing buildings with air intakes below grade, at ground level, or wall-mounted outside secure areas, some protection can be gained with physical security measures (e.g., placing fencing, surveillance cameras, and motion detectors around the intakes to facilitate monitoring by security personnel). These measures can help prevent malicious acts, but are less effective than elevating the intakes, because ground level releases under certain conditions can enter the intakes from points outside the area fenced or under surveillance.

Figure 3-11  
Example of enclosing an  
existing vulnerable air  
intake



SOURCE: CDC/NIOSH, PUBLICATION NO. 2002-139, *GUIDANCE FOR PROTECTING BUILDING ENVIRONMENTS FROM AIRBORNE CHEMICAL, BIOLOGICAL, OR RADIOLOGICAL ATTACKS*, MAY 2002

- Physical security for mechanical rooms to prevent the direct introduction of hazardous materials into the system of ducts that distributes air to the building should be maintained. This includes locking and controlling the access to all mechanical rooms containing HVAC equipment.

- Public access to building roofs should be prevented. Access to the roof may allow entry to the building and access to air intakes and HVAC equipment (e.g., self-contained HVAC units, laboratory or bathroom exhausts) located on the roof. From a physical security perspective, roofs are like other entrances to the building and should be secured appropriately. Roofs with HVAC equipment should be treated like mechanical areas. Fencing or other barriers should restrict access from adjacent roofs.
- Access to building operation systems by outsiders should be restricted. A building staff member should escort maintenance workers throughout their service visit and should visually inspect their work before final acceptance of the service. Alternatively, building managers can ensure the reliability of pre-screened service personnel from a trusted contractor.
- Access to information on building operations (including mechanical, electrical, vertical transport, fire and life safety, security system plans and schematics, and emergency operations procedures) should be strictly controlled. Such information should be released to authorized personnel through the development of an access list and controlled copy numbering.
- To prevent widespread dispersion of a contaminant released within lobbies, mailrooms, and loading docks, their HVAC systems should be isolated and the areas maintained at a negative pressure relative to the rest of the building, but at positive pressure relative to the outdoors. Physical isolation of these areas (well-sealed floor to roof-deck walls, sealed wall penetrations) is critical to maintaining the pressure differential. It requires special attention to ensure airtight boundaries between these areas and adjacent spaces. In some building designs (those having lobbies with elevator access, for example), establishing a negative pressure differential presents a challenge. A qualified mechanical engineer can assist in determining if the recommended isolation is feasible for a given building.

- Large buildings usually have multiple HVAC zones, with each zone served by its own air handling unit and duct system. In practice, these zones are not completely separated if they are on the same floor. Air flows between zones through hallways, atria, and doorways that are normally left open. Isolating the separate HVAC zones minimizes the potential spread of an airborne hazard within a building, and reduces the number of people potentially exposed if an internal release occurs. Zone separation provides a limited benefit against an external release. It increases internal resistance to air movement that is produced by wind forces and chimney effect, therefore reducing the rate of infiltration. In essence, isolating zones divide the building into separate environments, limiting the effects of single release to an isolated portion of the building. Isolation of zones requires full-height walls between each zone and its adjacent zone and hallway.
- Consider “shelter-in-place” rooms or areas where people can congregate in the event of an outdoor release. The goal is to create areas where outdoor air infiltration is very low. Usually such rooms will be in the inner part of the building in an area with no exterior windows. The rooms should have doors that are effective at preventing airflow and should contain staging supplies such as duct tape and plastic to help further seal the areas from the hallways. Typically, restrooms are a bad choice, because they have exhaust ducts that lead directly to the outside. Opening and closing a conventional hinged door can pump large amounts of air into the room. If practical, replace the door with a code compliant sliding door to reduce this effect. Shelter-in-place is discussed in detail in Section 5.2.
- Many central HVAC systems have energy management and control systems that can regulate airflow and pressures within a building on an emergency response basis. Some fire alarm systems provide useful capabilities during CBR events. In some cases, the best response option (given sufficient warning) might be to shut off the building’s HVAC and exhaust system(s), thus avoiding the introduction of a CBR agent

from outside. In other cases, interior pressure and airflow control may prevent the spread of a CBR agent released in the building and/or ensure the safety of egress pathways. The decision to install emergency HVAC control options should be made in consultation with a qualified mechanical engineer who understands the ramifications of various HVAC operating modes on building operation and safety systems.

- HVAC control may not be appropriate in all emergency situations. Protection from CBR attacks depends upon the design and operation of the HVAC system and the nature of the CBR agent release. Lobbies, loading docks, and mailrooms might be provided with manually operated exhaust systems, activated by trained personnel to remove contaminants in the event of a known release, exhausting air to an appropriate area. Manipulation of the HVAC system could minimize the spread of an agent. If an HVAC control plan is pursued, building personnel should be trained to recognize a terrorist attack and know when to initiate the control measures. For example, emergency egress stairwells should remain pressurized (unless they are known to contain the CBR source). Other areas, such as laboratories, clean rooms, or pressure isolation rooms in hospitals, may need to remain ventilated. All procedures and training associated with the control of the HVAC system should be addressed in the building's Emergency Response Plan (ERP).
- Ducted returns offer limited access points to introduce a CBR agent. The return vents can be placed in conspicuous locations, reducing the risk of an agent being secretly introduced into the return system. Non-ducted return air systems commonly use hallways or spaces above suspended ceilings as a return-air path or plenum. CBR agents introduced at any location above the suspended ceiling in a ceiling plenum return system will probably migrate back to the HVAC unit and, without highly efficient filtration for the particular agent, redistribute it to occupied areas. Buildings should be designed to minimize interaction between air-

handling zones. This can be partially accomplished by limiting shared returns. Where ducted returns are not feasible or warranted, hold-down clips may be used for the accessible areas of suspended ceilings that serve as the return plenum. This issue is closely related to the isolation of lobbies and mailrooms, because shared returns are a common way for contaminants from these areas to disperse into the rest of the building. These modifications may be more feasible for new building construction or those undergoing major renovation.

- A rapid response, such as shutting down an HVAC system, may involve closing various dampers, especially those controlling the flow of outdoor air (in the event of an exterior CBR release). When the HVAC system is turned off, the building pressure compared to outdoors may still be negative, drawing outdoor air into the building via many leakage pathways, including the HVAC system. Consideration should be given to installing low leakage dampers to minimize this flow pathway. Damper leakage ratings are available as part of the manufacturer's specifications and range from ultra-low to normal categories. Assuming that there is some warning prior to a direct CBR release, the speed with which these dampers respond to a "close" instruction can also be important. From a protective standpoint, dampers that respond quickly are preferred over dampers that might take 30 seconds or more to respond.

#### **Emergency Plans, Training, and Procedures for HVAC Systems.**

All buildings should have current emergency plans to address fire, weather, and other types of emergencies. In light of past U.S. experiences with anthrax and similar threats, these plans should be updated to consider CBR attack scenarios and the associated procedures. Emergency plans should have procedures for communicating instructions to building occupants, identifying suitable shelter-in-place areas (if they exist), identifying appropriate use and selection of personal protective equipment (i.e., clothing, gloves, respirators), and directing emergency evacuations. Individuals developing emergency plans and procedures should recognize that there are fundamental differences



between chemical, biological, and radiological agents. In general, chemical agents will show a rapid onset of symptoms, while the response to biological and radiological agents will be delayed. Issues such as designated areas and procedures for chemical storage, HVAC control or shutdown, and communications with building occupants and emergency responders, should all be addressed. The plans should be as comprehensive as possible, but, as described earlier, protected by limited and controlled access. When appropriately developed, these plans, policies, and procedures can have a major impact upon occupant survivability in the event of a CBR release. Staff training, particularly for those with specific responsibilities during an event, is essential and should cover both internal and external events. Holding regularly scheduled practice drills, similar to the common fire drill, allows for plan testing, as well as occupant and key staff rehearsal of the plan, and increases the likelihood for success in an actual event. For protection systems in which HVAC control is done via the energy management and control system, emergency procedures should be exercised periodically to ascertain that the various control options work (and continue to work) as planned.

Periodic training of HVAC maintenance staff in system operations and maintenance should be conducted. This training should include the procedures to be followed in the event of a suspected CBR agent release. Training should also cover health and safety aspects for maintenance personnel, as well as the potential health consequences to occupants of poorly performing systems. Development of current, accurate HVAC diagrams and HVAC system labeling protocols should be addressed. These documents can be of great value in the event of a CBR release.

Procedures and preventive maintenance schedules should be implemented for cleaning and maintaining ventilation system components. Replacement filters, parts, etc., should be obtained from known manufacturers and examined prior to installation. It is important that ventilation systems be maintained and cleaned according to the manufacturer's specifications. To do this requires information on HVAC system performance, flow rates, damper

modulation and closure, sensor calibration, filter pressure loss, filter leakage, and filter change-out recommendations. These steps are critical to ensure that protection and mitigation systems, such as particulate filtration, operate as intended.

### **3.5 ELECTRICAL SYSTEMS**

The major security functions of the electrical system are to maintain power to essential building services, especially those required for life safety and evacuation; provide lighting and surveillance to deter criminal activities; and provide emergency communications. Thus, the operability of electrical systems is an important element for deferring terrorist attacks and can become a critical component for life safety systems after an attack. Designers should consider the following recommendations for buildings requiring high security:

- Emergency and normal electric panels, conduits, and switchgear should be installed separately, at different locations, and as far apart as possible. Electric distribution should be run from separate locations.
- Emergency generators should be located away from loading docks, entrances, and parking. More secure locations include the roof, protected grade level, and protected interior areas.
- Fuel tanks should be mounted near the generator, given the same protection as the emergency generator, and sized to store an appropriate amount of fuel. A battery and/or UPS could serve a smaller building or leased facility.
- Conduits and lines should be installed outside to allow a trailer-mounted generator to connect to the building's electrical system. If tertiary power is required, other methods include generators and feeders from alternative substations.
- Site lighting should be coordinated with the CCTV system.
- Emergency lighting should be provided in restrooms.
- Building access points should be illuminated to aid in threat detection.

- Self-contained battery lighting should be provided in stairwells and for exit signs.
- Suspending electrical conduits from the ceiling should be avoided.
- Adequate lighting of perimeters and parking areas should be provided to aid in visual surveillance and to support the use of physical security systems.

### 3.6 FIRE PROTECTION SYSTEMS

The fire protection system inside the building should maintain life safety protection after an incident and allow for safe evacuation of the building when appropriate. Although fire protection systems are designed to perform well during fires, they are not traditionally designed to survive bomb blasts. To enhance the performance of fire protection systems, especially in the case of an explosive blast, the designer should consider the following:

- The fire protection water system should be protected from single-point failure in case of a blast event. The incoming line should be encased, buried, or located 50 feet away from high-risk areas. The interior mains should be looped and sectionalized.
- To increase the reliability of the fire protection system in strategic locations, a dual pump arrangement should be considered, with one electric pump and one diesel pump. The pumps should be located away from each other.
- All security locking arrangements on doors used for egress must comply with requirements of the National Fire Protection Association (NFPA) 101, Life Safety Code.

### 3.7 COMMUNICATIONS SYSTEMS

For buildings requiring greater protection, the designer should consider the following:

- **Redundant communications.** The facility could have a second telephone service to maintain communications in

case of an incident. A base radio communication system with antenna should be installed in the stairwell, and portable sets distributed on floors. This is the preferred alternative.

- **Radio telemetry.** Distributed antennas could be located throughout the facility if required for emergency communications through wireless transmission of data.
- **Alarm and information systems.** Alarm and information systems should not be collected and mounted in a single conduit, or even collocated. Circuits to various parts of the building should be installed in at least two directions and/or risers. Low voltage signal and control copper conductors should not share conduits with high voltage power conductors. Fiber-optic conductors are generally preferred over copper.
- **Empty conduits.** Empty conduits and power outlets can be provided for future installation of security control equipment.
- **Mass notification.** All inhabited buildings should have a timely means to notify occupants of threats and give instructions as to responses. Building communications systems should provide real-time notification of occupants and passersby in the immediate vicinity of the building during emergency situations. The information relayed should be specific enough to determine the appropriate response actions.

### 3.8 ELECTRONIC SECURITY SYSTEMS

Electronic security, including surveillance, intrusion detection, and screening, is a key element of facility protection. Many aspects of electronic security and the posting of security personnel have been adequately dealt with in other criteria and guideline documents. These criteria primarily address access control design, including stair and lobby design, because access control must be considered when design concepts for a building are first conceived. Although fewer options are available for modernization projects, some designs can be altered to consider future access control objectives.

The purpose of electronic security is to improve the reliability and effectiveness of life safety systems, security systems, and building functions. When possible, accommodations should be made for future developments in security systems.

This chapter is not a design guide for Electronic Security Systems (ESS). The following criteria are only intended to stress those concepts and practices that warrant special attention to enhance public safety. Consult design guides pertinent to the specific project for detailed information about electronic security. A description of Electronic Security Systems is provided in Appendix D.

For control centers and building management systems, designers should consider the following:

- The Operational Control Center (OCC), Fire Command Center (FCC), and Security Control Center (SCC) may be collocated. If collocated, the chain of command should be carefully pre-planned to ensure the most qualified leadership is in control for specific types of events. Secure information links should be provided between the OCC, FCC, and SCC.
- A Backup Control Center (BCC) should be provided in a different location, such as a manager's or engineer's office. If feasible, an off-site location should be considered.
- A fully redundant BCC should be installed (this is an alternative to the above).
- Basic intrusion detection devices should be provided: magnetic reed switches for interior doors and openings, glass break sensors for windows up to scalable heights, and balanced magnetic contact switch sets for all exterior doors, including overhead/roll-up doors. Roof intrusion detection should be reviewed.
- Monitoring should be done at an off-site facility.
- An on-site monitoring center should be used during normal business hours and be operational 24 hours.

- A color CCTV surveillance system with recording capability should be provided to view and record activity at the perimeter of the building, particularly at primary entrances and exits. A mix of monochrome cameras should be considered for areas that lack adequate illumination for color cameras.

The following considerations apply when lighting systems are intended to support CCTV assessment or surveillance: field of view of the camera; lighting intensity levels; maximum light-to-dark ratio; scene reflectance; daylight-to-darkness transitions; camera mounting systems relative to lighting; spectral response of the camera; cold-start time; and restrike time.

### 3.9 ENTRY-CONTROL STATIONS

Entry-control stations should be provided at main perimeter entrances where security personnel are present (see Figure 3-12). In addition, entry-control stations should be located close to the pe-



Figure 3-12 Physical security devices

perimeter entrance to permit people inside the station to maintain constant surveillance over the entrance and its approaches. Additional considerations at entry-control stations include:

- A holding area for unauthorized vehicles or those needing further inspection should be established. A turnaround area should be provided so that traffic is not impeded.
- Control measures such as displaying a decal on the window or having a specially marked vehicle should be established.
- Entry-control stations that are manned 24 hours each day should have interior and exterior lighting, interior heating and cooling (where appropriate), and a sufficient glassed area to afford adequate observation for people inside. Where appropriate, entry-control stations should be designed for optimum personnel ID and movement control. Each station should include a telephone, a radio, and badge racks (if required).
- Signs should be erected to assist in controlling authorized entry, to deter unauthorized entry, and to preclude accidental entry. Signs should be plainly displayed and legible from any approach to the perimeter from a reasonable distance. The size and coloring of a sign, its letters, and the interval of posting must be appropriate to each situation.
- Entry-control stations should be hardened against attacks according to the type of threat. The methods of hardening may include:
  - Reinforced concrete or masonry
  - Steel plating
  - Bullet-resistant glass
  - Commercially fabricated, bullet-resistant building components or assemblies

### **3.10 PHYSICAL SECURITY SYSTEMS**

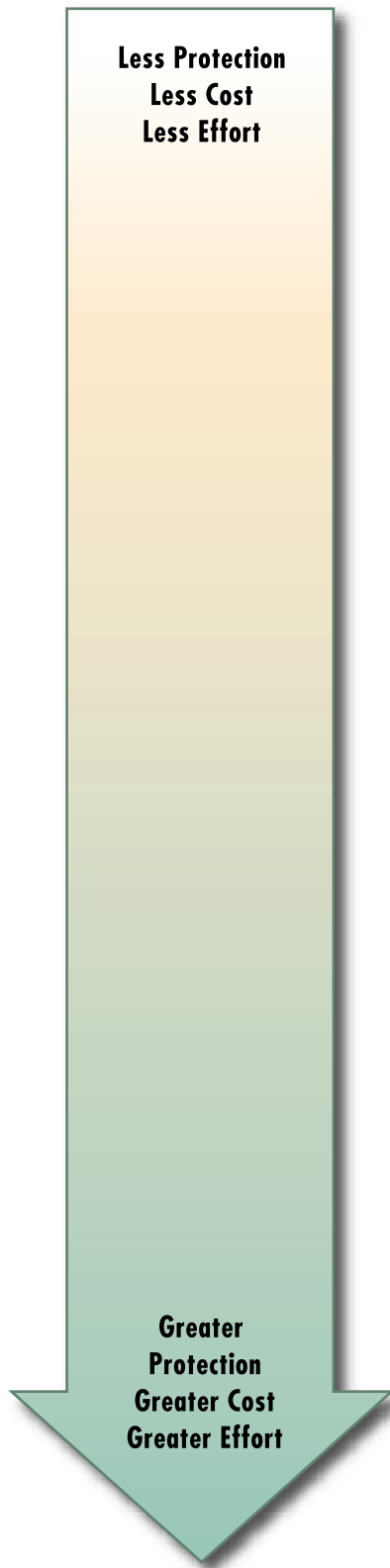
Physical security concerns the physical measures designed to safeguard people; prevent unauthorized access to equipment, installations, material, and documents; and safeguard against terrorist attacks. As such, all security operations face new and complex physical security challenges across the full spectrum of operations. Challenges relative to physical security include the control of populations, information dominance, multi-national and interagency connectivity, antiterrorism, and the use of physical security assets as a versatile force multiplier.

The rapid evolution of physical security equipment technology leads to physical security challenges, which are exponentially multiplied by the introduction of the information age (see Appendix D). Physical security challenges must be understood, and measures must be taken to minimize them to enhance the protection of people within a facility.

#### **3.11 SUMMARY OF BUILDING ENVELOPE MITIGATION MEASURES**

A general spectrum of building envelope mitigation measures ranging from the least protection, cost, and effort going to the greatest protection, cost, and effort is provided below. Detailed discussions of individual measures can be found earlier in the chapter. Please note this is a nominal ranking of mitigation measures. In practice, the effectiveness and cost of individual mitigation measures may deviate from this example based on specific applications.





- Ensure that exterior doors into inhabited areas open outward. Ensure emergency exit doors only facilitate exiting.
- Secure roof access hatches from the interior. Prevent public access to building roofs.
- Restrict access to building operation systems.
- Conduct periodic training of HVAC operations and maintenance staff.
- Evaluate HVAC control options.
- Install empty conduits for future security control equipment during initial construction or major renovation.
- Do not mount plumbing, electrical fixtures, or utility lines on the inside of exterior walls.
- Minimize interior glazing near high-risk areas.
- Establish emergency plans, policies, and procedures.
- Establish written plans for evacuation and sheltering in place.
- Illuminate building access points.
- Restrict access to building information.
- Secure HVAC intakes and mechanical rooms.
- Limit the number of doors used for normal entry/egress.
- Lock all utility access openings.
- Provide emergency power for emergency lighting in restrooms, egress routes, and any meeting room without windows.
- Install an internal public address system.
- Stagger interior doors and offset interior and exterior doors.
- Eliminate hiding places.
- Install a second and separate telephone service.
- Install radio telemetry distributed antennas throughout the facility.
- Use a badge identification system for building access.
- Install a CCTV surveillance system.
- Install an electronic security alarm system.
- Install rapid response and isolation features into HVAC systems.
- Use interior barriers to differentiate levels of security.
- Locate utility systems away from likely areas of potential attack.
- Install call buttons at key public contact areas.

Continued on next page



**Less Protection  
Less Cost  
Less Effort**

**Greater  
Protection  
Greater Cost  
Greater Effort**

- Install emergency and normal electric equipment at different locations.
- Avoid exposed structural elements.
- Reinforce foyer walls.
- Use architectural features to deny contact with exposed primary vertical load members.
- Isolate lobbies, mailrooms, loading docks, and storage areas.
- Locate stairwells remotely. Do not discharge stairs into lobbies, parking, or loading areas.
- Elevate HVAC fresh-air intakes.
- Create "shelter-in-place" rooms or areas.
- Separate HVAC zones. Eliminate leaks and increase building air tightness.
- Install blast-resistant doors or steel doors with steel frames.
- Physically separate unsecured areas from the main building.
- Install HVAC exhausting and purging systems.
- Connect interior non-load bearing walls to structure with non-rigid connections.
- Use structural design techniques to resist progressive collapse.
- Treat exterior shear walls as primary structures.
- Orient glazing perpendicular to the primary façade facing uncontrolled vehicle approaches.
- Use reinforced concrete wall systems in lieu of masonry or curtain walls.
- Ensure active fire system is protected from single-point failure in case of a blast event.
- Install a Backup Control Center (BCC).
- Avoid eaves and overhangs or harden to withstand blast effects.
- Establish ground floor elevation 4 feet above grade.
- Avoid re-entrant corners on the building exterior.

**T**his chapter discusses blast effects, building damage, injuries, levels of protection, stand-off distance, and predicting blast effects. Specific blast design concerns and mitigation measures are discussed in Chapters 2 and 3. Explosive events have historically been a favorite tactic of terrorists for a variety of reasons and this is likely to continue into the future. Ingredients for homemade bombs are easily obtained on the open market as are the techniques for making bombs. Also, explosive events are easy and quick to execute. Vehicle bombs have the added advantage of being able to bring a large quantity of explosives to the doorstep of the target undetected. Finally, terrorists often attempt to use the dramatic component of explosions, in terms of the sheer destruction they cause, to generate media coverage in hopes of transmitting their political message to the public. The DoD, GSA, and DOS have considerable experience with blast effects and blast mitigation. However, many architects and building designers do not have such experience. For additional information on explosive blast, see FEMA 427, *Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks*.

## **4.1 BLAST EFFECTS**

When a high order explosion is initiated, a very rapid exothermic chemical reaction occurs. As the reaction progresses, the solid or liquid explosive material is converted to very hot, dense, high-pressure gas. The explosion products initially expand at very high velocities in an attempt to reach equilibrium with the surrounding air, causing a shock wave. A shock wave consists of highly compressed air, traveling radially outward from the source at supersonic velocities. Only one-third of the chemical energy available in most high explosives is released in the detonation process. The remaining two-thirds is released more slowly as the detonation products mix with air and burn. This afterburning process has little effect on the initial blast wave because it occurs much slower than the original detonation. However, later stages of the blast wave can be affected by the afterburning, particularly

for explosions in confined spaces. As the shock wave expands, pressures decrease rapidly (with the cube of the distance) because of geometric divergence and the dissipation of energy in heating the air. Pressures also decay rapidly over time (i.e., exponentially) and have a very brief span of existence, measured typically in thousandths of a second, or milliseconds. An explosion can be visualized as a “bubble” of highly compressed air that expands until reaching equilibrium with the surrounding air.

Explosive detonations create an incident blast wave, characterized by an almost instantaneous rise from atmospheric pressure to a peak overpressure. As the shock front expands pressure decays back to ambient pressure, a negative pressure phase occurs that is usually longer in duration than the positive phase as shown in Figure 4-1. The negative phase is usually less important in a design than the positive phase.

When the incident pressure wave impinges on a structure that is not parallel to the direction of the wave’s travel, it is reflected and reinforced, producing what is known as reflected pressure. The

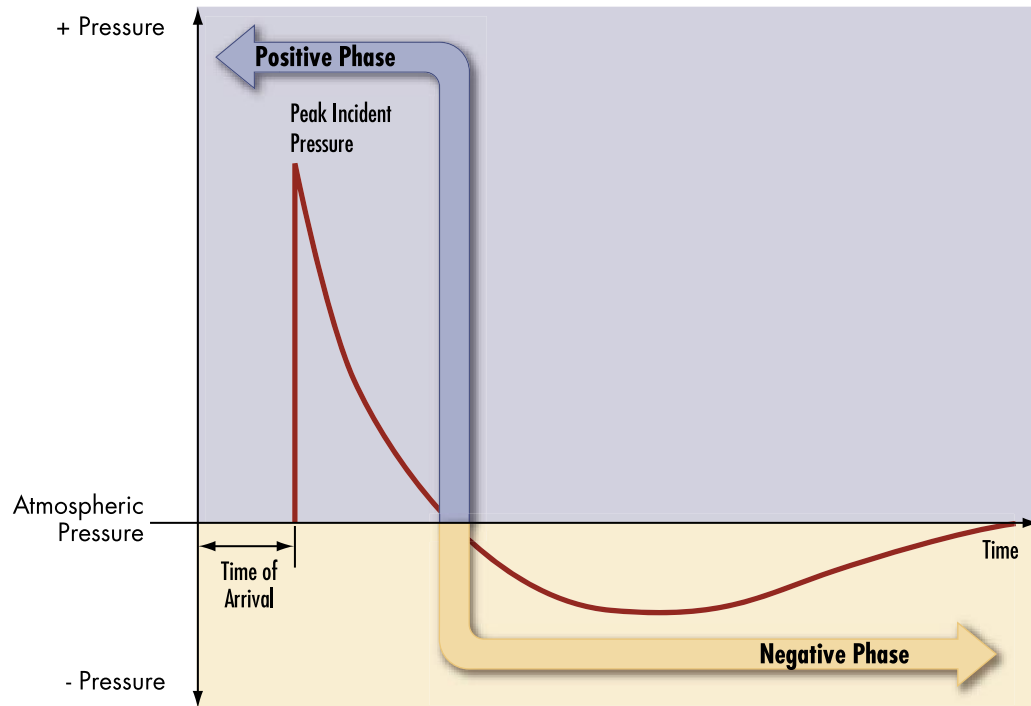


Figure 4-1 Typical pressure-time history

reflected pressure is always greater than the incident pressure at the same distance from the explosion. The reflected pressure varies with the angle of incidence of the shock wave. When the shock wave impinges on a surface that is perpendicular to the direction it is traveling, the point of impact will experience the maximum reflected pressure. When the reflecting surface is parallel to the blast wave, the minimum reflected pressure or incident pressure will be experienced. In addition to the angle of incidence, the magnitude of the peak reflected pressure is dependent on the peak incident pressure, which is a function of the net explosive weight and distance from the detonation.

Figure 4-2 shows typical reflected pressure coefficients versus the angle of incidence for four different peak incident pressures. The reflected pressure coefficient equals the ratio of the peak reflected pressure to the peak incident pressure ( $Cr = Pr / Pi$ ). This figure shows that reflected pressures for explosive detonations

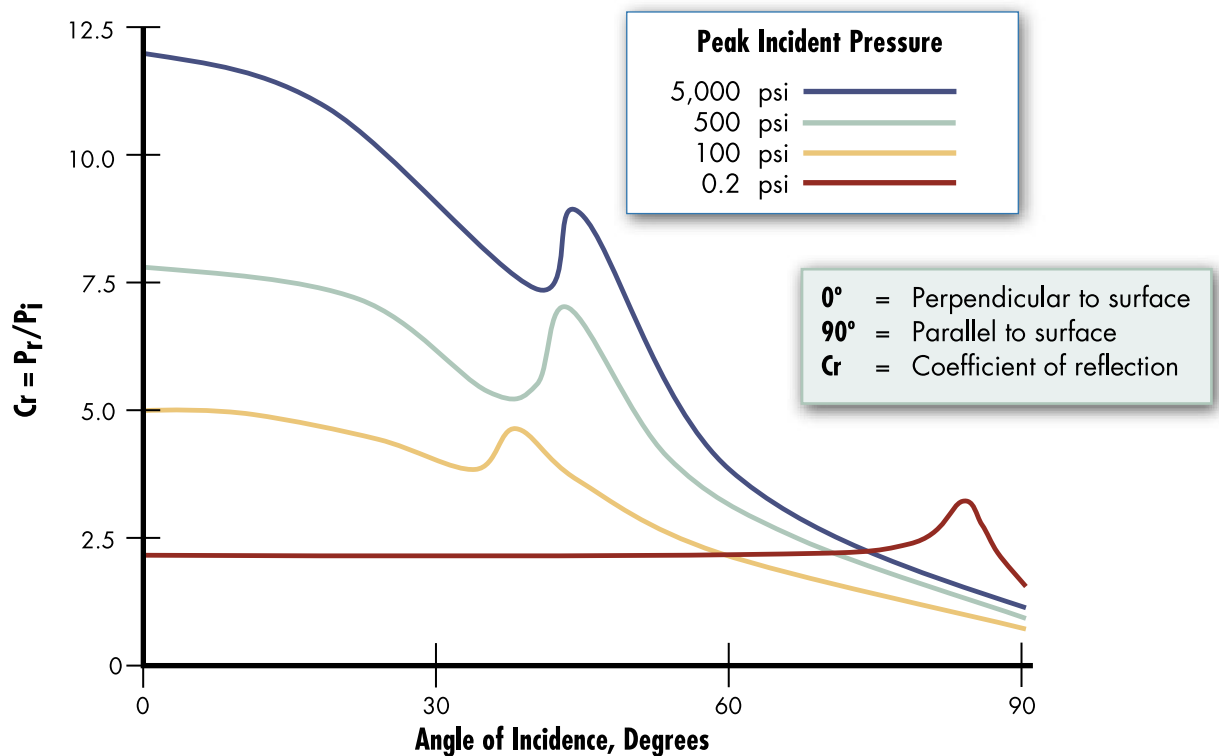


Figure 4-2 Reflected pressure coefficient vs. angle of incidence

can be almost 13 times greater than peak incident pressures and, for all explosions, the reflected pressure coefficients are significantly greater closer to the explosion.

The integrated area under the pressure verse time function is known as the impulse:

$$I = \int P(t) dt$$

I = impulse (psi-ms or Mpa-ms)

P = Pressure (psi or MPa)

T = time (ms)

Impulse is a measure of the energy from an explosion imparted to a building. Both the negative and positive phases of the pressure-time waveform contribute to impulse. Figure 4-3 shows how impulse and pressure vary over time from a typical explosive detonation. The magnitude and distribution of blast loads on a structure vary greatly with several factors:

- Explosive properties (type of material, energy output, and quantity of explosive)

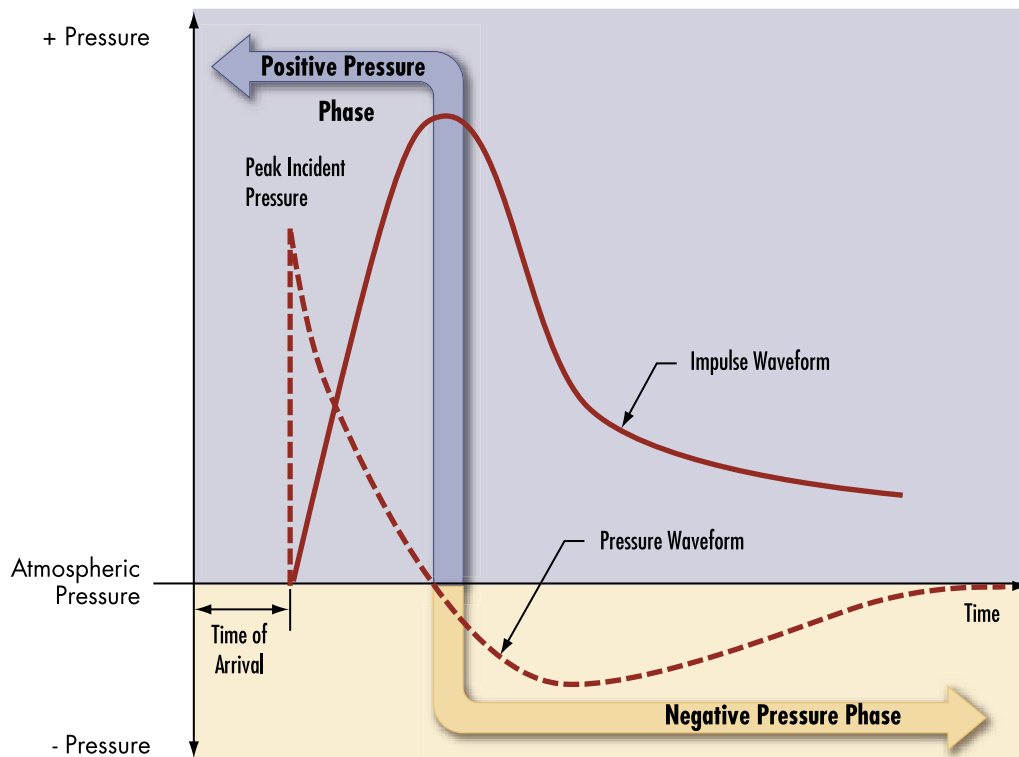


Figure 4-3 Typical impulse waveform

- Location of the detonation relative to the structure
- Reinforcement of the pressure pulse through its interaction with the ground or structure (reflections)

The reflected pressure and the reflected impulse are the forces to which the building ultimately responds. These forces vary in time and space over the exposed surface of the building, depending on the location of the detonation in relation to the building. Therefore, when analyzing a structure for a specific blast event, care should be taken to identify the worst case explosive detonation location.

In the context of other hazards (e.g., earthquakes, winds, or floods), an explosive attack has the following distinguishing features:

- The intensity of the pressures acting on a targeted building can be several orders of magnitude greater than these other hazards. It is not uncommon for the peak incident pressure to be in excess of 100 psi on a building in an urban setting for a vehicle weapon parked along the curb. At these pressure levels, major damages and failure are expected.
- Explosive pressures decay extremely rapidly with distance from the source. Therefore, the damages on the side of the building facing the explosion may be significantly more severe than on the opposite side. As a consequence, direct air-blast damages tend to cause more localized damage. In an urban setting, however, reflections off surrounding buildings can increase damages to the opposite side.
- The duration of the event is very short, measured in thousandths of a second, or milliseconds. This differs from earthquakes and wind gusts, which are measured in seconds, or sustained wind or flood situations, which may be measured in hours. Because of this, the mass of the structure has a strong mitigating effect on the response because it takes time to mobilize the mass of the structure. By the time the mass is mobilized, the loading is gone, thus mitigating the response.

This is the opposite of earthquakes, whose imparted forces are roughly in the same timeframe as the response of the building mass, causing a resonance effect that can worsen the damage.

#### **4.1.1 Building Damage**

The extent and severity of damage and injuries in an explosive event cannot be predicted with perfect certainty. Past events show that the unique specifics of the failure sequence for a building significantly affect the level of damage. Despite these uncertainties, it is possible to give some general indications of the overall level of damage and injuries to be expected in an explosive event, based on the size of the explosion, distance from the event, and assumptions about the construction of the building.

Damage due to the air-blast shock wave may be divided into direct air-blast effects and progressive collapse. Direct air-blast effects are damage caused by the high-intensity pressures of the air-blast close in to the explosion and may induce the localized failure of exterior walls, windows, floor systems, columns, and girders. A discussion of progressive collapse can be found in Chapter 3.

The air blast shock wave is the primary damage mechanism in an explosion. The pressures it exerts on building surfaces may be several orders of magnitude greater than the loads for which the building is designed. The shock wave also acts in directions that the building may not have been designed for, such as upward on the floor system. In terms of sequence of response, the air-blast first impinges on the weakest point in the vicinity of the device closest to the explosion, typically the exterior envelope of the building. The explosion pushes on the exterior walls at the lower stories and may cause wall failure and window breakage. As the shock wave continues to expand, it enters the structure, pushing both upward and downward on the floors (see Figure 4-4).

Floor failure is common in large-scale vehicle-delivered explosive attacks, because floor slabs typically have a large surface area for the pressure to act on and a comparably small thickness. In terms



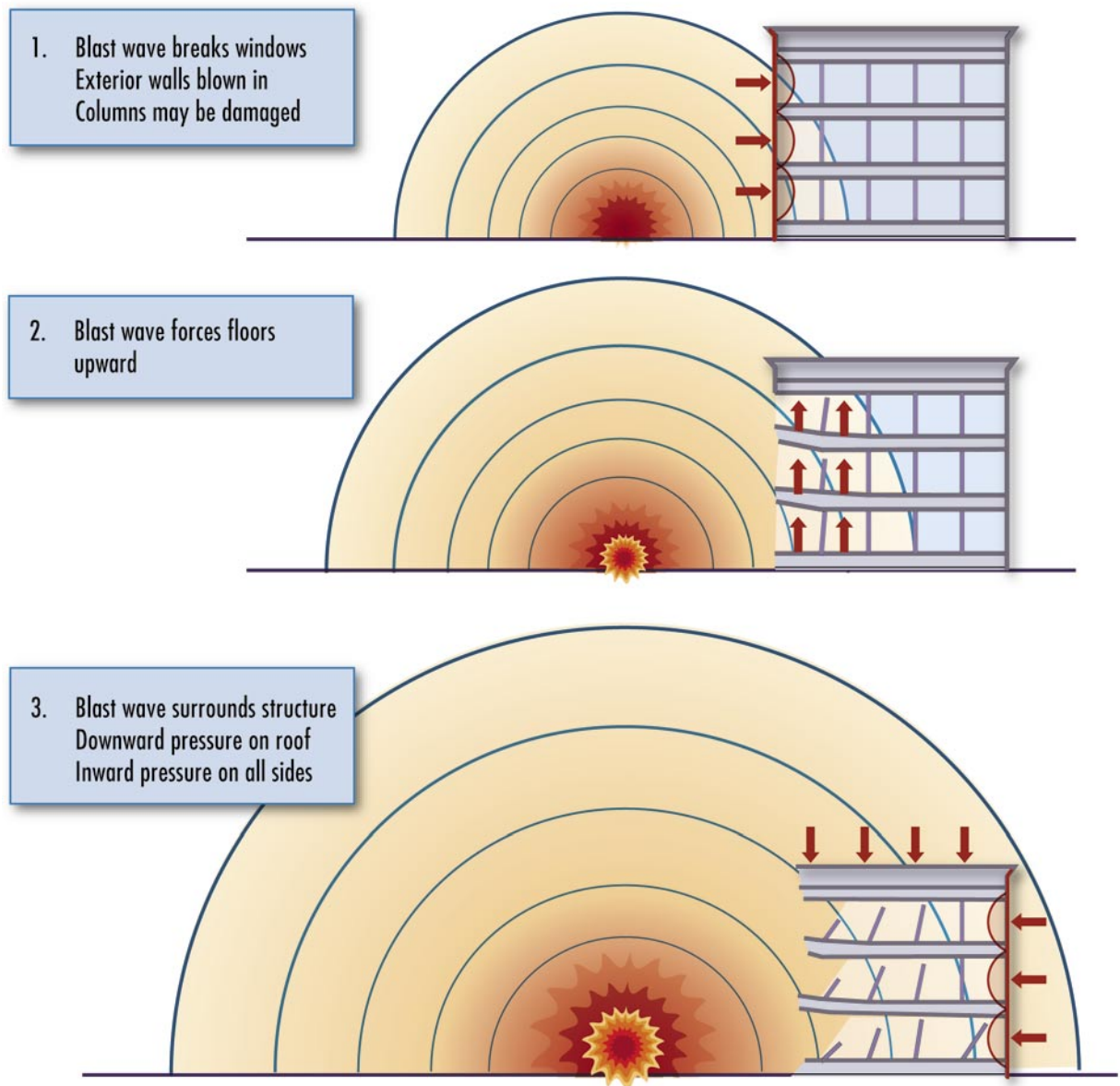


Figure 4-4 Blast pressure effects on a structure

SOURCE: NAVAL FACILITIES ENGINEERING SERVICE CENTER, *USER'S GUIDE ON PROTECTION AGAINST TERRORIST VEHICLE BOMBS*, MAY 1998

of the timing of events, the building is engulfed by the shock wave and direct air-blast damage occurs within tens to hundreds of milliseconds from the time of detonation. If progressive collapse is initiated, it typically occurs within seconds.

Glass is often the weakest part of a building, breaking at low pressures compared to other components such as the floors, walls, or columns. Past incidents have shown that glass breakage may extend for miles in large external explosions. High-velocity glass fragments have been shown to be a major contributor to injuries in such incidents. For incidents within downtown city areas, falling glass poses a major hazard to passersby on the sidewalks below and prolongs post-incident rescue and cleanup efforts by leaving tons of glass debris on the street. Specific glazing design considerations are discussed in Chapter 3.

#### **4.1.2 Injuries**

Severity and type of injury patterns incurred in explosive events may be related to the level of structural damage. The high pressure of the air-blast that enters through broken windows can cause eardrum damage and lung collapse. As the air-blast damages the building components in its path, missiles are generated that cause impact injuries. Airborne glass fragments typically cause penetration or laceration-type injuries. Larger fragments may cause non-penetrating, or blunt trauma, injuries. Finally, the air-blast pressures can cause occupants to be bodily thrown against objects or to fall. Lacerations due to high-velocity flying glass fragments have been responsible for a significant portion of the injuries received in explosion incidents. In the bombing of the Murrah Federal Building in Oklahoma City, for instance, 40 percent of the survivors in the Murrah Federal Building cited glass as contributing to their injuries. Within nearby buildings, laceration estimates ranged from 25 percent to 30 percent.

#### **4.1.3 Levels of Protection**

The amount of explosive and the resulting blast dictate the level of protection required to prevent a building from collapsing or minimizing injuries and deaths. Table 4-1 shows how the DoD correlates levels of protection with potential damage and expected injuries. The GSA and the Interagency Security Committee (ISC) also use the level of protection concept. However, wherein the DoD has five levels, they have established four levels of protection.

Table 4-1: DoD Minimum Antiterrorism (AT) Standards for New Buildings\*

Level of Protection	Potential Structural Damage	Potential Door and Glazing Hazards	Potential Injury
<b>Below AT standards</b>	Severely damaged. Frame collapse/ massive destruction. Little left standing.	Doors and windows fail and result in lethal hazards	Majority of personnel suffer fatalities.
<b>Very Low</b>	Heavily damaged - onset of structural collapse. Major deformation of primary and secondary structural members, but progressive collapse is unlikely. Collapse of non-structural elements.	Glazing will break and is likely to be propelled into the building, resulting in serious glazing fragment injuries, but fragments will be reduced. Doors may be propelled into rooms, presenting serious hazards.	Majority of personnel suffer serious injuries. There are likely to be a limited number (10 percent to 25 percent) of fatalities.
<b>Low</b>	Damaged – unrepairable.  Major deformation of non-structural elements and secondary structural members, and minor deformation of primary structural members, but progressive collapse is unlikely.	Glazing will break, but fall within 1 meter of the wall or otherwise not present a significant fragment hazard. Doors may fail, but they will rebound out of their frames, presenting minimal hazards.	Majority of personnel suffer significant injuries. There may be a few (<10 percent) fatalities.
<b>Medium</b>	Damaged – repairable.  Minor deformations of non-structural elements and secondary structural members and no permanent deformation in primary structural members.	Glazing will break, but will remain in the window frame. Doors will stay in frames, but will not be reusable.	Some minor injuries, but fatalities are unlikely.
<b>High</b>	Superficially damaged.  No permanent deformation of primary and secondary structural members or non-structural elements.	Glazing will not break. Doors will be reusable.	Only superficial injuries are likely.

\* THE DoD UNIFIED FACILITIES CRITERIA (UFC), *DoD MINIMUM ANTITERRORISM STANDARDS FOR BUILDINGS*, UFC 4-010-01 31 JULY 2002

The GSA and ISC levels of protection can be found in GSA PBS-P100, *Facilities Standards for the Public Buildings Service*, November 2000, Section 8.6.

The levels of protection above can roughly be correlated for conventional construction without any blast hardening to the incident pressures shown in Table 4-2.

Table 4-2: Correlation of DoD Level of Protection to Incident Pressure

Level of Protection	Incident Pressure (psi)
High	1.1
Medium	1.8
Low	2.3

Figure 4-5 shows an example of a range-to-effect chart that indicates the distance or stand-off to which a given size bomb will produce a given effect (see Section 4.2). This type of chart can be used to display the blast response of a building component or window at different levels of protection. It can also be used to consolidate all building response information to assess needed actions if the threat weapon-yield changes. For example, an amount of explosives are stolen and indications are that they may be used against a specific building. A building-specific range-to-effect chart will allow quick determination of the needed stand-off for the amount of explosives in question, after the explosive weight is converted to TNT equivalence.

Research performed as part of the threat assessment process should identify bomb sizes used in the locality or region. Security consultants have valuable information that may be used to evaluate the range of likely charge weights. Given an explosive weight and a

stand-off distance, Figure 4-5 can be used to predict damage for nominal building construction.

Figures 4-6 and 4-7 show blast effects predictions for a building based on a typical car bomb and a typical large truck bomb detonated in the

For design purposes, large-scale truck bombs typically contain 10,000 pounds or more of TNT equivalent, depending on the size and capacity of the vehicle used to deliver the weapon. Vehicle bombs that utilize vans down to small sedans typically contain 4,000 to 500 pounds of TNT equivalent, respectively. A briefcase bomb is approximately 50 pounds, and a pipe bomb is generally in the range of 5 pounds of TNT equivalent.

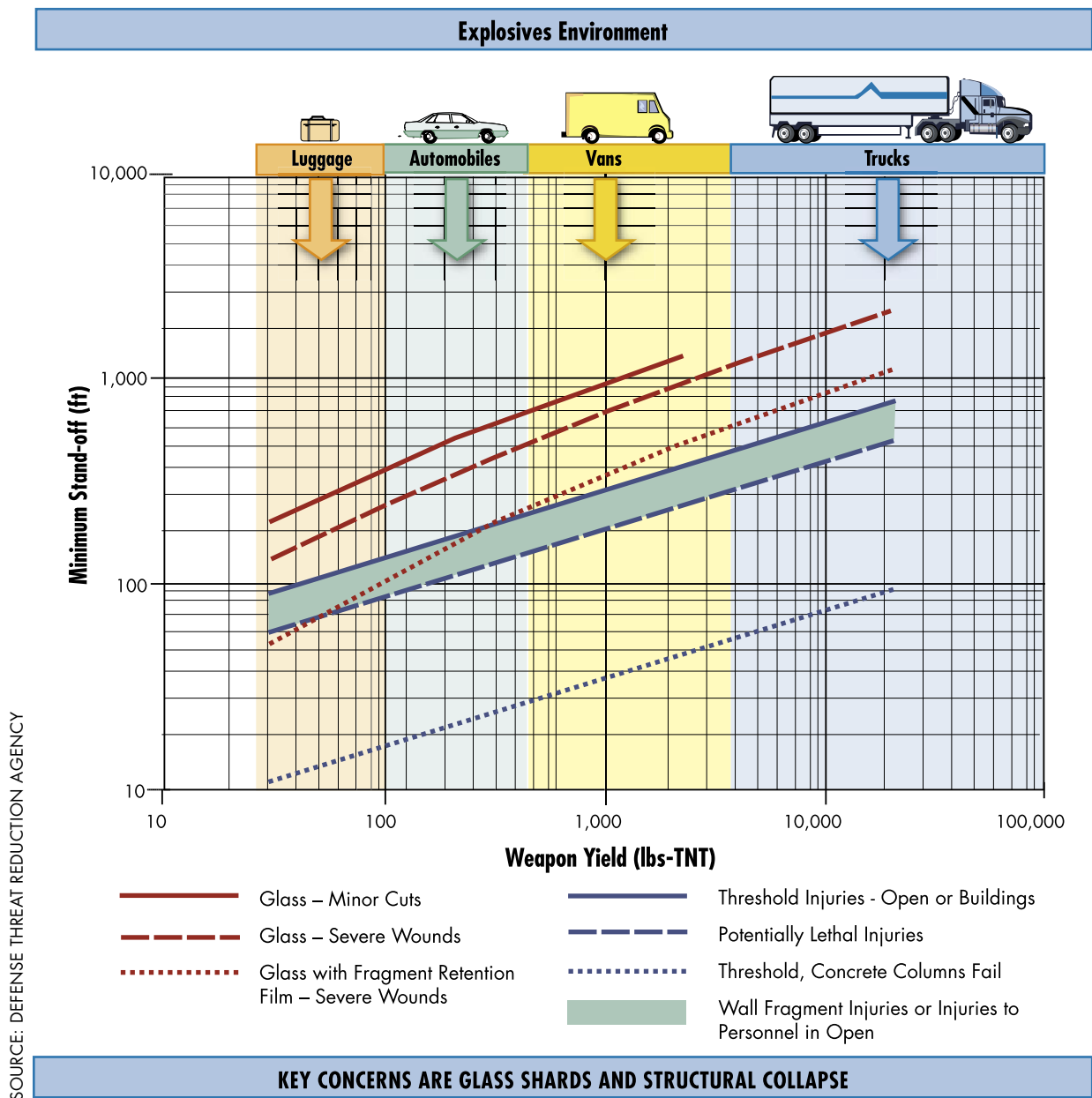


Figure 4-5 Explosives environments - blast range to effects

building's parking lot, respectively. A computer-based Geographic Information System (GIS) was used to analyze the building's vehicular access and circulation pattern to determine a reasonable detonation point for a vehicle bomb. Structural blast analysis was then performed using nominal explosive weights and a nominal building structure. The results are shown in Figures 4-6 and 4-7.



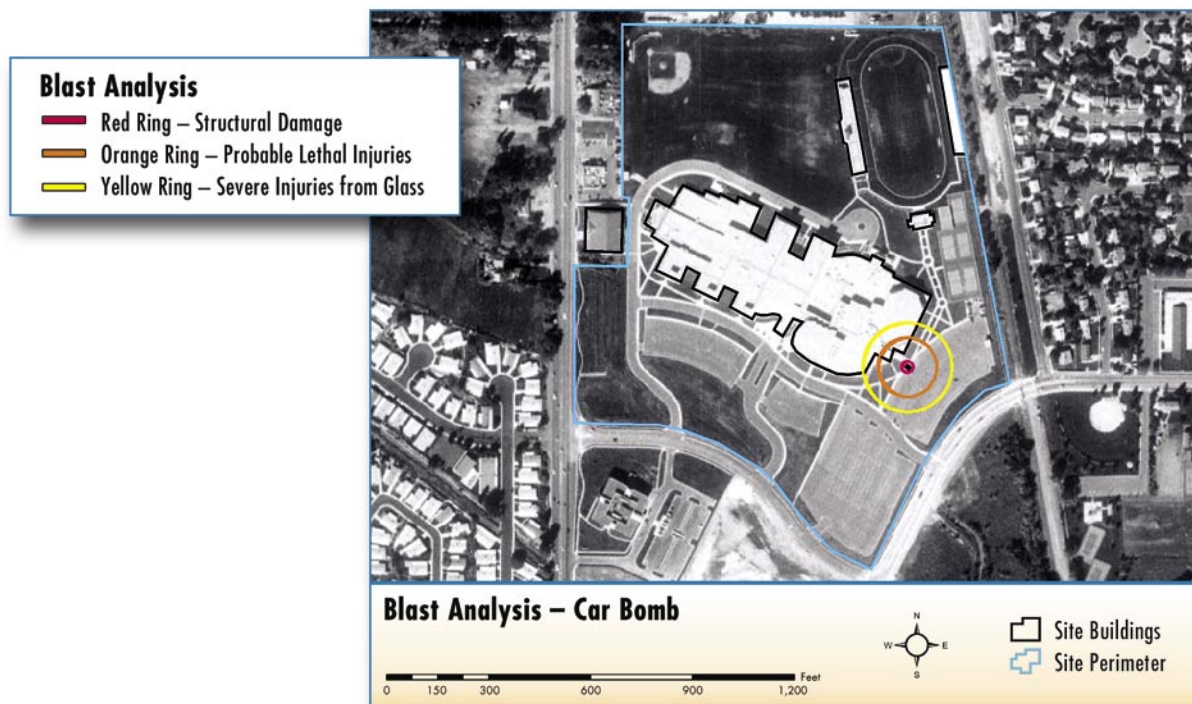


Figure 4- 6 Blast analysis of a building for a typical car bomb detonated in the building's parking lot

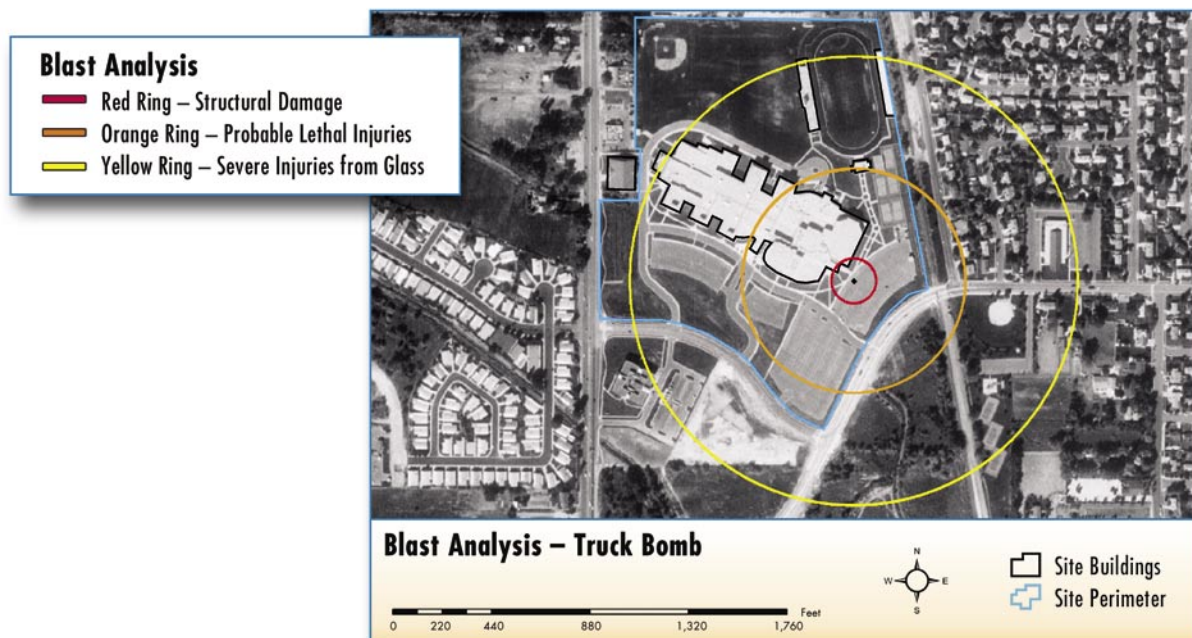


Figure 4-7 Blast analysis of a building for a typical large truck bomb detonated in the building's parking lot

The red ring indicates the area in which structural collapse is predicted. The orange and yellow rings indicate predictions for lethal injuries and severe injuries from glass, respectively. Please note that nominal inputs were used in this analysis and they are not a predictive examination.

In the case of a stationary vehicle bomb, knowing the size of the bomb (TNT equivalent in weight), its distance from the structure, how the structure is put together, and the materials used for walls, framing, and glazing allows the designer to determine the level of damage that will occur and the level of protection achieved. Whether an existing building or a new construction, the designer can then select mitigation measures as presented in this chapter and in Chapters 2 and 3 to achieve the level of protection desired.

## 4.2 STAND-OFF DISTANCE AND THE EFFECTS OF BLAST

Energy from a blast decreases rapidly over distance. In general, the cost to provide asset protection will decrease as the distance between an asset and a threat increases, as shown in Figure 4-8. However, increasing stand-off also requires more land and more perimeter to secure with barriers, resulting in an increased

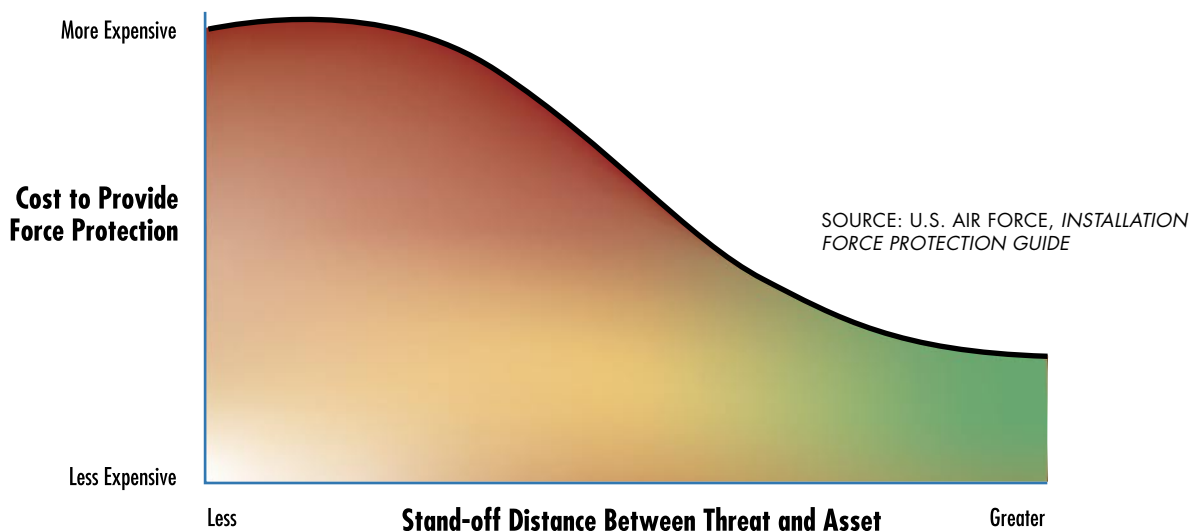


Figure 4-8 Relationship of cost to stand-off distance

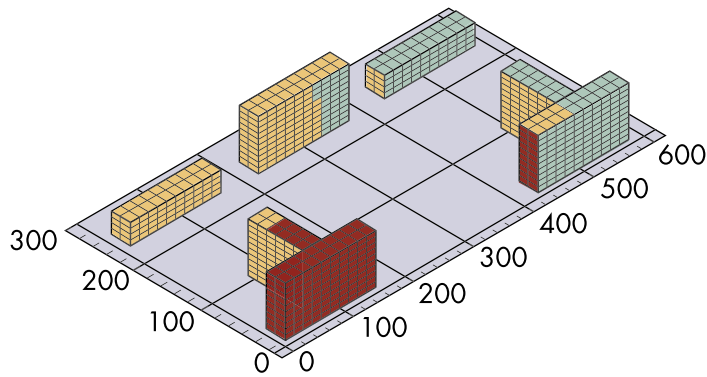
hardening necessary to provide the required level of protection decreases. Figure 4-9 shows how the impact of a blast will decrease as the stand-off distance increases, as indicated in the blast analysis of the Khobar Towers incident. Increasing the stand-off distance from 80 to 400 feet would have significantly limited the damage to the building and hazard to occupants, the magnitude of which is shown as the yellow and red areas in Figure 4-9. Additional concepts of stand-off distance are discussed in Section 2.3.

The critical location of the weapon is a function of the site, the building layout, and the security measures in place. For vehicle bombs, the critical locations are considered to be at the closest point that a vehicle can approach on each side, assuming that all security measures are in place. Typically, this is a vehicle parked along the curb directly outside the building, or at the entry control point where inspection takes place. For internal weapons, location is dictated by the areas of the building that are publicly accessible (e.g., lobbies, corridors, auditoriums, cafeterias, or gymnasiums). Range or stand-off is measured from the center of gravity of the charge located in the vehicle or other container to the building component under consideration.

Defining appropriate stand-off distance for a given building component to resist explosive blast effects is difficult. Often, in urban settings, it is either not possible or practical to obtain appropriate stand-off distance. Adding to the difficulty is the fact that defining appropriate stand-off distance requires a prediction of the explosive weight of the weapon. In the case of terrorism, this is tenuous at best.

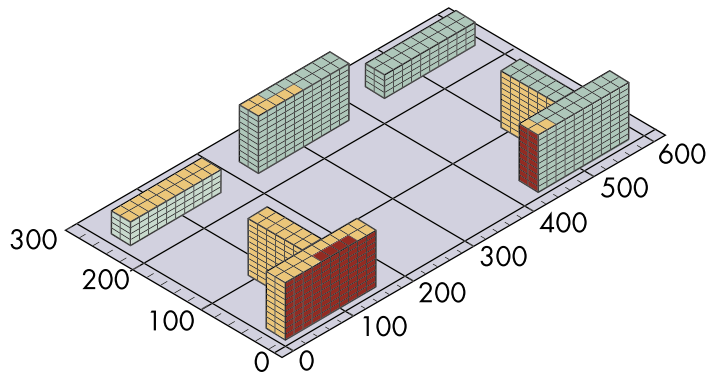
The DoD prescribes minimum stand-off distances based on the required level of protection. Where minimum stand-off distances are met, conventional construction techniques can be used with some modifications. In cases where the minimum stand-off cannot be achieved, the building must be hardened to achieve the required level of protection (see Unified Facilities Criteria – DoD Minimum Antiterrorism Standards for Buildings, UFC 4-010-01, 31 July 2002).





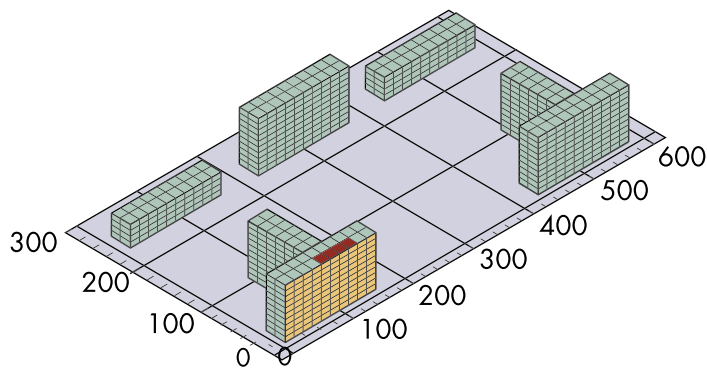
### Detonation at 80 feet from Building 131

This is the actual stand-off that was provided at the Khobar Towers Complex



### Detonation at 170 feet from Building 131

This is the minimum stand-off recommended by FMS-114 Engineer Operations Short of War



### Detonation at 400 feet from Building 131

This stand-off distance would have prevented serious damage and reduced the extent of casualties

COLOR	DAMAGE DESCRIPTION	HAZARD TO OCCUPANTS
<b>RED</b>	Very severe damage, possible collapse	Very high hazard, widespread death and serious injury likely
<b>YELLOW</b>	Very unrepairable structural damage	High hazard, death and serious injury possible
<b>GREEN</b>	Moderate Repairable structural damage	Medium hazard, limited casualties and injury possible

Figure 4-9 Stand-off distance and its relationship to blast impact as modeled on the Khobar Towers site

The GSA and ISC Security Criteria do not require or mandate specific stand-off distances. Rather, they provide protection performance criteria. In order to economically meet these performance standards, they present recommended stand-off distances for vehicles that are parked on adjacent properties and for vehicles that are parked on the building site (see *GSA Security Criteria, Draft Revision*, October 8, 1997, and *ISC Security Design Criteria for New Federal Office Buildings and Major Modernization Projects*, May 28, 2001).

Site and layout design guidance as well as specific mitigation measures to enhance stand-off and enhance protection from explosive blast are discussed in Chapter 2.

## **4.3 PREDICTING BLAST EFFECTS**

### **4.3.1 Blast Load Predictions**

The first step in predicting blast effects on a building is to predict blast loads on the structure. For a detonation that is exterior to a building, it is the blast pressure pulse that causes damage to the building. Because the pressure pulse varies based on stand-off distance, angle of incidence, and reflected pressure over the exterior of the building, the blast load prediction should be performed at multiple threat locations; however, worse case conditions are normally used for decision-making.

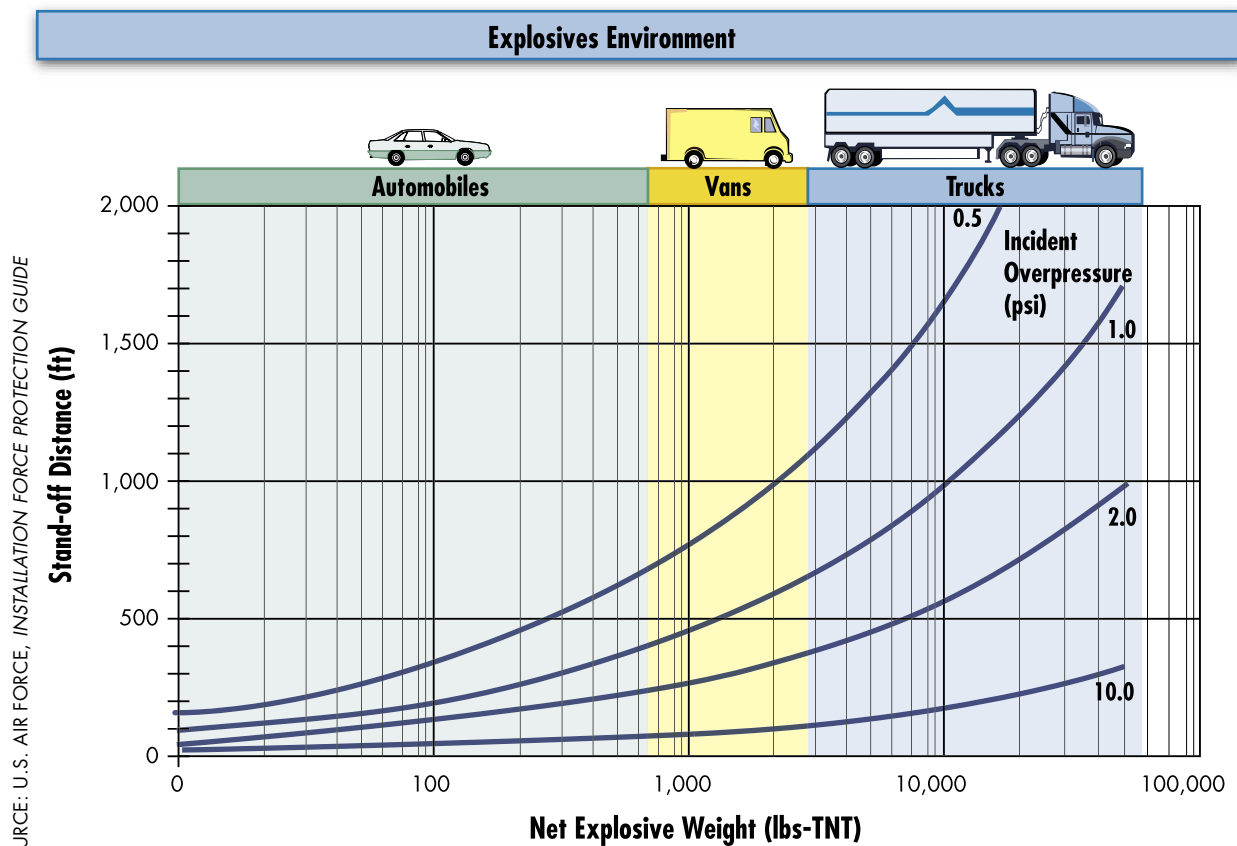
For complex structures requiring refined estimates of blast load, blast consultants may use sophisticated methods such as Computational Fluid Dynamics (CFD) computer programs to predict blast loads. These complex programs require special equipment and training to run.

In most cases, especially for design purposes, more simplified methods may be used by blast consultants to predict blast loads. The overpressure is assumed to instantaneously rise to its peak value and decay linearly to zero in a time known as the duration time. In order to obtain the blast load, a number of different tools can be used. Tables of pre-determined values may be used (see *GSA Security Reference Manual: Part 3 – Blast Design & Assess-*

ment Guidelines, July 31, 2001) or computer programs may be used, such as:<sup>1</sup>

- ATBLAST (GSA)
- CONWEP (U.S. Army Engineer Research and Development Center)

Figure 4-10 provides a quick method for predicting the expected overpressure (expressed in pounds per square inch or psi) on a building for a specific explosive weight and stand-off distance. Enter the x-axis with the estimated explosive weight a terrorist might use and the y-axis with a known stand-off distance from a building. By correlating the resultant effects of overpressure with



SOURCE: U.S. AIR FORCE, INSTALLATION FORCE PROTECTION GUIDE

Figure 4-10 Incident overpressure measured in pounds per square inch, as a function of stand-off distance and net explosive weight (pounds-TNT)

<sup>1</sup>For security reasons, the distribution of these computer programs is limited.

other data, the degree of damage that the various components of a building might receive can be estimated. The vehicle icons in Figures 4-5 and 4-10 indicate the relative size of the vehicles that might be used to transport various quantities of explosives.

### **4.3.2 Blast Effects Predictions**

After the blast load has been predicted, damage levels may be evaluated by explosive testing, engineering analysis, or both. Explosive testing is actively conducted by Federal Government agencies such as the Defense Threat Reduction Agency, DOS, and GSA. Manufacturers of innovative products also conduct explosive test programs to verify the effectiveness of their products.

Often, testing is too expensive an option for the design community and an engineering analysis is performed instead. To accurately represent the response of an explosive event, the analysis needs to be time dependent and account for non-linear behavior.

Non-linear dynamic analysis techniques are similar to those currently used in advanced seismic analysis. Analytical models range from equivalent single-degree-of-freedom (SDOF) models to finite element (FEM) representation. In either case, numerical computation requires adequate resolution in space and time to account for the high-intensity, short-duration loading and non-linear response. The main problems are the selection of the model, the appropriate failure modes, and, finally, the interpretation of the results for structural design details. Whenever possible, results are checked against data from tests and experiments on similar structures and loadings. Available computer programs include:

- AT Planner (U.S. Army Engineer Research and Development Center)
- BEEM (Technical Support Working Group)
- BLASTFX (Federal Aviation Administration)

Components such as beams, slabs, or walls can often be modeled by a SDOF system. The response can be found by using the charts

developed by Biggs and military handbooks. For more complex elements, the engineer must resort to numerical time integration techniques. The time and cost of the analysis cannot be ignored in choosing analytical procedures. SDOF models are suitable for numerical analysis on PCs and micro-computers, but the most sophisticated FEM systems (with non-linear material models and options for explicit modeling of reinforcing bars) may have to be carried out on mainframes. Because the design analysis process is a sequence of iteration, the cost of analysis must be justified in terms of benefits to the project and increased confidence in the reliability of the results. In some cases, an SDOF approach will be used for the preliminary design and a more sophisticated approach, using finite elements, will be used for the final design.

Table 4-3 provides estimates of incident pressures at which damage may occur.

Table 4-3: Damage Approximations

Damage	Incident Overpressure (psi)
Typical window glass breakage	0.15 – 0.22
Minor damage to some buildings	0.5 – 1.1
Panels of sheet metal buckled	1.1 – 1.8
Failure of concrete block walls	1.8 – 2.9
Collapse of wood framed buildings	Over 5.0
Serious damage to steel framed buildings	4 – 7
Severe damage to reinforced concrete structures	6 – 9
Probable total destruction of most buildings	10 – 12

SOURCE: *EXPLOSIVE SHOCKS IN AIR*, KINNEY & GRAHM, 1985; *FACILITY DAMAGE AND PERSONNEL INJURY FROM EXPLOSIVE BLAST*, MONTGOMERY & WARD, 1993; AND *THE EFFECTS OF NUCLEAR WEAPONS*, 3RD EDITION, GLASSTONE & DOLAN, 1977

**Additional sources of information:**

- **Air Force Engineering and Services Center.** *Protective Construction Design Manual*, ESL-TR-87-57. Prepared for Engineering and Services Laboratory, Tyndall Air Force Base, FL. (1989).
- **U.S. Department of the Army.** *Fundamentals of Protective Design for Conventional Weapons*, TM 5-855-1. Washington, DC, Headquarters, U.S. Department of the Army. (1986).
- **U.S. Department of the Army.** *Security Engineering*, TM 5-853 and Air Force AFMAN 32-1071, Volumes 1, 2, 3, and 4. Washington, DC, Departments of the Army and Air Force. (1994).
- **U.S. Department of the Army.** *Structures to Resist the Effects of Accidental Explosions*, Army TM 5-1300, Navy NAVFAC P-397, AFR 88-2. Washington, DC, Departments of the Army, Navy, and Air Force. (1990).
- **U.S. Department of Energy.** *A Manual for the Prediction of Blast and Fragment Loading on Structures*, DOE/TIC 11268. Washington, DC, Headquarters, U.S. Department of Energy. (1992).
- **U.S. General Services Administration.** *GSA Security Reference Manual: Part 3 Blast Design and Assessment Guidelines*. (2001).
- **Biggs, John M.** *Introduction to Structural Dynamics*. McGraw-Hill. (1964).
- **The Institute of Structural Engineers.** *The Structural Engineer's Response to Explosive Damage*. SETO, Ltd., 11 Upper Belgrave Street, London SW1X8BH. (1995).
- **Mays, G.S. and Smith, P.D.** *Blast Effects on Buildings: Design of Buildings to Optimize Resistance to Blast Loading*. Thomas Telford Publications, 1 Heron Quay, London E14 4JD. (1995).
- **National Research Council.** *Protecting Buildings from Bomb Damage*. National Academy Press. (1995).

**T**his chapter is based on guidance from the CDC/NIOSH and the DoD and presents protective measures and actions to safeguard the occupants of a building from CBR threats. Evacuation, sheltering in place, personal protective equipment, air filtration and pressurization, and exhausting and purging will be discussed, as well as CBR detection<sup>1</sup>. Additionally, CBR design mitigation measures are discussed in Chapter 3 and Appendix C contains a glossary of CBR terms and a summary of CBR agent characteristics.

Recent terrorist events have increased interest in the vulnerability of buildings to CBR threats. Of particular concern are building HVAC systems, because they can become an entry point and distribution system for airborne hazardous contaminants. Even without special protective systems, buildings can provide protection in varying degrees against airborne hazards that originate outdoors. Conversely, the hazards produced by a release inside a building can be much more severe than a similar release outdoors. Because buildings allow only a limited exchange of air between indoors and outdoors, not only can higher concentrations occur when there is a release inside, but hazards may persist longer indoors.

After the presence of an airborne hazard is detected, there are five possible protective actions for a building and its occupants. In increasing order of complexity and cost, these actions are:

1. Evacuation
2. Sheltering in Place
3. Personal Protective Equipment
4. Air Filtration and Pressurization
5. Exhausting and Purging

<sup>1</sup>This chapter includes a number of protective measures that are included for informational purposes only. It is not the intention of FEMA to endorse any particular product or protective measure.

These actions are implemented, singly or in combination, when a hazard is present or known to be imminent. To ensure these actions will be effective, a protective-action plan specific to each building, as well as training and familiarization for occupants, is required. Exhausting and purging is listed last because it is usually the final action after any airborne hazard incident.

## **5.1 EVACUATION**

Evacuation is the most common protective action taken when an airborne hazard, such as smoke or an unusual odor, is perceived in a building. In most cases, existing plans for fire evacuation apply. Orderly evacuation is the simplest and most reliable action for an internal airborne hazard. However, it may not be the best action in all situations, especially in the case of an external CBR release or plume, particularly one that is widespread. If the area covered by the plume is too large to rapidly and safely exit, sheltering in place should be considered. If a CBR agent has infiltrated the building and evacuation is deemed not to be safe, the use of protective hoods may be appropriate. Two considerations in non-fire evacuation are: 1) to determine if the source of the airborne hazard is internal or external, and 2) to determine if evacuation may lead to other risks. Also, evacuation and assembly of occupants should be on the upwind side of the building and at least 100 feet away, because any airborne hazard escaping the building will be carried downwind.

## **5.2 SHELTERING IN PLACE**

In normal operations, a building does little to protect occupants from airborne hazards outside the building because outdoor air must be continuously introduced to provide a comfortable, healthy indoor environment. However, a building can provide substantial protection against agents released outdoors if the flow of fresh air is filtered/cleaned, or temporarily interrupted or reduced. Interrupting the flow of fresh air is the principle applied in the protective action known as sheltering in place.



The advantage of sheltering in place is that it can be implemented rapidly. The disadvantage is that its protection is variable and diminishes with the duration of the hazard. Sheltering requires that two distinct actions be taken without delay to maximize the passive protection a building provides:

- First, reduce the indoor-outdoor air exchange rate before the hazardous plume arrives. This is achieved by closing all windows and doors, and turning off all fans, air conditioners, and combustion heaters.
- Second, increase the indoor-outdoor air exchange rate as soon as the hazardous plume has passed. This is achieved by opening all windows and doors, and turning on all fans to ventilate the building.

The level of protection that can be attained by sheltering in place is substantial, but it is less than can be provided by high efficiency filtration of the fresh air introduced into the building. The amount of protection varies with:

- **The building's air exchange rate.** The tighter the building (i.e., the lower the air exchange rate), the greater the protection it provides. In most cases, air conditioners and combustion heaters cannot be operated while sheltering in place because operating them increases the indoor-outdoor exchange of air.
- **The duration of exposure.** Protection varies with time, diminishing as the time of exposure increases. Sheltering in place is, therefore, suitable only for exposures of short duration, roughly 2 hours or less, depending on conditions.
- **Purging or period of occupancy.** How long occupants remain in the building after the hazardous plume has passed also affects the level of protection. Because the building slowly purges contaminants that have entered it, at some point during plume passage, the concentration inside exceeds the concentration outside. Maximum protection is attained by

increasing the air exchange rate after plume passage or by exiting the building into clean air.

- **Natural filtering.** Some filtering occurs when the agent is deposited in the building shell or upon interior surfaces as air passes into and out of the building. The tighter the building, the greater the effect of this natural filtering.

In a home, taking the actions required for sheltering (i.e., closing windows and doors, and turning off all air conditioners, fans, and combustion heaters) is relatively simple. Doing so in a commercial or apartment building may require more time and planning. All air handling units must be turned off and any dampers for outside air must be closed. Procedures for a protective action plan, therefore, should include:

- Identifying all air handling units, fans, and the switches needed to deactivate them.
- Identifying cracks, seams, joints, and pores in the building envelope to be temporarily sealed to further reduce outside air infiltration. Keeping emergency supplies, such as duct tape and polyethylene sheeting, on hand.
- Identifying procedures for purging after an internal release (i.e., opening windows and doors, turning on smoke fans, air handlers, and fans that were turned off) to exhaust and purge the building.
- Identifying sheltering rooms (i.e., interior rooms having a lower air exchange rate) that may provide a higher level of passive protection. It may be desirable to go to a predetermined sheltering room (or rooms) and:
  - Shut and lock all windows and doors
  - Seal any windows and vents with plastic sheeting and duct tape

- Seal the door(s) with duct tape around the top, bottom, and sides
- Firmly pack dampened towels along the bottom of each door
- Turn on a TV or radio that can be heard within the shelter and listen for further instructions
- When the “all clear” is announced, open windows and doors

Important considerations for use of sheltering in place are that stairwells must be isolated by closed fire doors, elevators must not be used, and clear evacuation routes must remain open if evacuation is required. Escape hoods may be needed if the only evacuation routes are through contaminated areas.

One final consideration for sheltering in place is that occupants cannot be forced to participate. It is important to develop a plan in cooperation with likely participants and awareness training programs that include discussions of sheltering in place and events (CBR attacks, hazardous material releases, or natural disasters) that might make sheltering preferable to evacuation. During an event, some building protective action plans call for making a concise information announcement, and then giving occupants 3 to 5 minutes to proceed to the sheltering area or evacuate the building before it is sealed. Training programs and information announcements during an event should be tailored to help occupants to make informed decisions.

### **5.3 PERSONAL PROTECTIVE EQUIPMENT**

A wide range of individual protection equipment is available, including respirators, protective hoods, protective suits, CBR detectors, decontamination equipment, etc. The DOJ, National Institute of Justice (NIJ), *Guide for the Selection of Personal Protective Equipment for Emergency First Responders* (NIJ Guide 102-00, Volumes I-IV) provides summarizes and evaluates a wide range of personal protective equipment. The U.S. Joint Service Materiel

Group (JSMG) has sponsored the Nuclear Biological Chemical (NBC) Industry Group to produce a catalogue of CBR products and services manufactured and provided by companies in the United States.

Of particular note, new models of universal-fit escape hoods have been developed for short-duration “escape-only” wear to protect against chemical agents, aerosols (including biological agents), and some toxic industrial chemicals. These hoods are compact enough to be stored in desks or to be carried on the belt. They should be stored in their sealed pouches and opened only when needed. Most of these hoods form protective seals at the neck and do not require special fitting techniques or multiple sizes to fit a large portion of the population. Training is required to use the hoods

properly. Depending on hood design, the wearer must breathe through a mouth bit or use straps to tighten a nose cup around the nose and mouth (see Figure 5-1).

The protective capability and shelf life of these hoods varies with the design. The filters of the hoods contain both high efficiency particulate air (HEPA) filters and packed carbon beds, so they will remove chemical and biological aerosols, as well as chemical vapors and gases. Although the carbon filters are designed to filter a broad range of toxic chemicals, they cannot filter all chemicals. An important consideration in planning for use of escape hoods is that their filters are not effective against certain chemicals of high vapor pressure. Chemical masks provide no protection against carbon monoxide, which is produced in fires. Manufacturers’ data should be



SOURCE: MSA INTERNATIONAL

Figure 5-1 Universal-fit escape hood

checked closely when ordering. Other escape hoods are available that employ compressed oxygen cylinders, rather than air filters, to provide eye and respiratory protection for very short periods.

There are no government standards for hoods intended for protection against the malicious use of chemical or biological agents. In selecting an escape hood, a purchaser should, therefore, require information on laboratory verification testing. Plans should be made for training, fitting, storing, and maintaining records relative to storage life, and there should be procedures for instructing building occupants as to when to put on the hoods. Wearing a mask can cause physiological strain and may cause panic or stress that could lead to respiratory problems in some people. Finally, it should be recognized that no single selection of personal protective equipment is effective against every possible threat. Selection must be tied to specific threat/hazard characteristics.

## **5.4 AIR FILTRATION AND PRESSURIZATION**

Among the various protective measures for buildings, high efficiency air filtration/cleaning provides the highest level of protection against an outdoor release of hazardous materials. It can also provide continuous protection, unlike other approaches for which protective measures are initiated upon detecting an airborne hazard.

Two basic methods of applying air filtration to a building are external filtration and internal filtration. External filtration involves drawing air from outside, filtering and/or cleaning it, and discharging the air inside the building or protected zone. This provides the higher level of protection, but involves substantially higher costs. Internal filtration involves drawing air from inside the building, filtering and/or cleaning it, and discharging the air back inside the building.

The relative levels of protection of the two methods can be illustrated in terms of protection factor, and the ratio of external dose and internal dose (concentration integrated over time). External filtration systems with high efficiency filters can yield protection

factors greater than 100,000. For internal filtration, the protection factors are likely to be less and are highly variable. The protection of internal filtration varies with a number of factors, including those listed in sheltering in place, the efficiency of the filter, flow rate of the filter unit, and size of the room or building in which the filter unit operates.

#### 5.4.1 Air Filtration and Cleaning Principles

Air filtration is the removal of particulate contaminants from the air. Air cleaning is the removal of gases or vapors from the air. The collection mechanisms for these two types of systems are very different.

**Particulate Air Filters.** Particulate air filters consist of fibrous materials (see Figure 5-2), which capture aerosols. Their efficiency will depend on the size of the aerosol, the type of filter, the velocity of the air, and the type of microbe. The basic principle of particulate air filtration is not to restrict the passage of particles

by the gap between fibers, but by altering the airflow streamlines. The airflow will slip around the fiber, but higher density aerosols and particulates will not change direction as rapidly.

Four different collection mechanisms govern particulate air filter performance: inertial impaction, interception, diffusion, and electrostatic attraction (see Figure 5-3). The first three mechanisms are the most important for mechanical filters and are influenced by particle size. Impaction occurs when a particle in an air stream passing around a filter

Airborne contaminants can be gases, vapors, or aerosols (small solid and liquid particles). Most biological and radiological agents are aerosols, whereas most chemical warfare agents are gaseous.



Figure 5-2 Scanning electron microscope image of a polyester-glass fiber filter

SOURCE: CDC/NIOSH PUBLICATION NO. 2003-136, *GUIDANCE FOR FILTRATION AND AIR CLEANING SYSTEMS TO PROTECT BUILDING ENVIRONMENTS FROM AIRBORNE CHEMICAL, BIOLOGICAL, OR RADIOLOGICAL ATTACKS*, APRIL 2003

fiber, because of its inertia, deviates from the air stream and collides with a fiber. Interception occurs when a particle in the air stream passing around filter fibers comes in contact with a fiber because of its size. Impaction and interception are dominant for large particles ( $> 0.2$  microns). Diffusion occurs when the random (Brownian) motion of a particle causes that particle to contact a fiber. Diffusion is the dominant collection mechanism for smaller particles ( $< 0.2$  microns). The combined effect of these three collection mechanisms results in the classic collection efficiency curve that is shown in Figure 5-4. The fourth mechanism, electrostatic attraction, plays a minor role in mechanical filtration because, after fiber contact is made, small particles are retained on the fibers by a weak electrostatic force.

Electrostatically enhanced filters are different from electrostatic precipitators, also known as electronic air cleaners. Electrostatic precipitators require electrical power and charged plates to attract and capture particles. In electrostatic filters, the electrostatically enhanced fibers actually attract the particles to the fibers, in addition to retaining them. Electrostatic filters use polarized fibers to increase the collection efficiency, typically have less packing density, and consequently will have a much lower pressure drop than a similar efficiency mechanical filter.

Particulate air filters are classified as mechanical filters or electrostatic filters. As a mechanical filter loads with particles over time, its collection efficiency and pressure drop typically in-

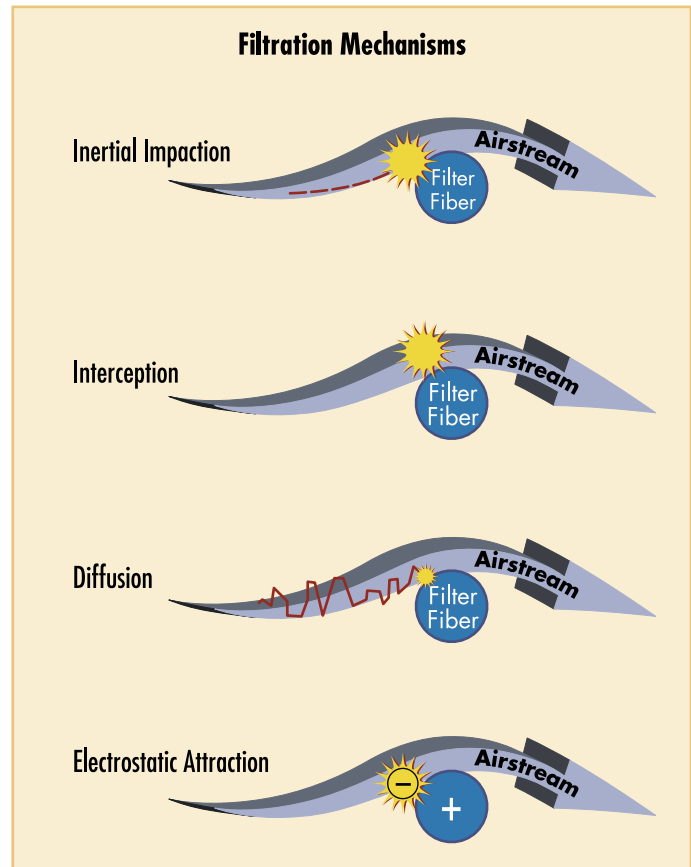


Figure 5-3 Four primary filter collection mechanisms

SOURCE: CDC/NIOSH PUBLICATION NO. 2003-136, *GUIDANCE FOR FILTRATION AND AIR CLEANING SYSTEMS TO PROTECT BUILDING ENVIRONMENTS FROM AIRBORNE CHEMICAL, BIOLOGICAL, OR RADIOLOGICAL ATTACKS*, APRIL 2003



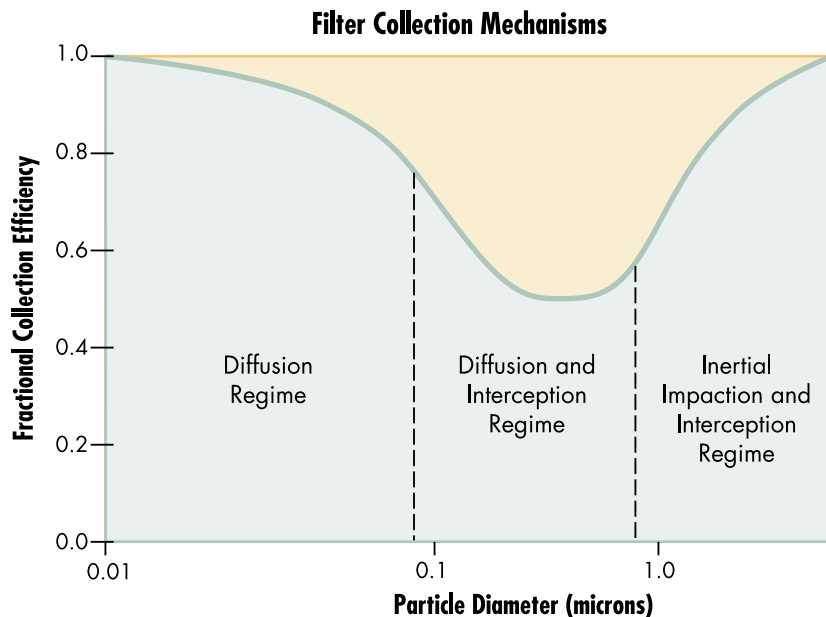


Figure 5-4 Classic collection efficiency curve

SOURCE: CDC/NIOSH PUBLICATION NO. 2003-136, *GUIDANCE FOR FILTRATION AND AIR CLEANING SYSTEMS TO PROTECT BUILDING ENVIRONMENTS FROM AIRBORNE CHEMICAL, BIOLOGICAL, OR RADIOLOGICAL ATTACKS*, APRIL 2003

crease. The pressure drop caused by particulate air filters must be taken into account in HVAC system design. Higher capacity fan units may be needed to overcome increased resistance caused by higher efficiency filters. Eventually, the increased pressure drop significantly inhibits airflow, and the filters must be replaced. For this reason, pressure drop across mechanical filters is often monitored because it indicates when to replace filters. Conversely, electrostatic filters may lose their

collection efficiency over time when exposed to certain chemicals, aerosols, or high relative humidities. Pressure drop in an electrostatic filter generally increases at a slower rate than it does in a mechanical filter of similar efficiency. Thus, unlike the mechanical filter, pressure drop for the electrostatic filter is a poor indicator of the need to change filters. Periodic aerosol measurements may be appropriate to verify their performance. When selecting an HVAC filter, the differences between mechanical and electrostatic filters will have an impact on the filter's performance (collection efficiency over time), as well as on maintenance requirements (change-out schedules).

Particulate air filters are commonly rated based on their collection efficiency, pressure drop (airflow resistance), and particulate holding capacity. Two filter-rating systems are currently used in the United States, the American Society of Heating, Refrigerating, and Air-conditioning Engineers (ASHRAE) Standard 52.1-1992 and ASHRAE Standard 52.2-1999. Standard 52.1 mea-



sures arrestance, dust spot efficiency, and dust holding capacity. Arrestance refers to a filter's ability to capture a mass fraction of coarse test dust and is better suited for describing low- and medium-efficiency filters. Dust spot efficiency measures a filter's ability to remove particles that tend to soil the interior of buildings. Arrestance values may be high even for low efficiency filters, and may not adequately differentiate the effectiveness of different filters for CBR protection. Dust holding capacity is a measure of the total amount of dust a filter is able to hold during a dust-loading test.

ASHRAE Standard 52.2 measures particle size efficiency (PSE). This newer standard is a more descriptive test, which quantifies filtration efficiency in different particle size ranges and is more applicable in determining a filter's effectiveness to capture a specific agent. Standard 52.2 reports the particle size efficiency results as a minimum efficiency reporting value (MERV) rating between 1 and 20. A higher MERV rating indicates a more efficient filter. The standard provides a table (see Table 5-1) showing minimum PSE for three size ranges for each of the MERV numbers 1 through 16. Thus, if the size of a contaminant is known, an appropriate filter with the desired PSE for that particular particle size can be identified.

A wide variety of particulate air filters are available to meet many specialized needs. They range from the low efficiency dust filters, such as roll-type filters used in commercial buildings, to HEPA and ultra low penetration air (ULPA) filters used in clean rooms and operating rooms (see Figure 5-5).

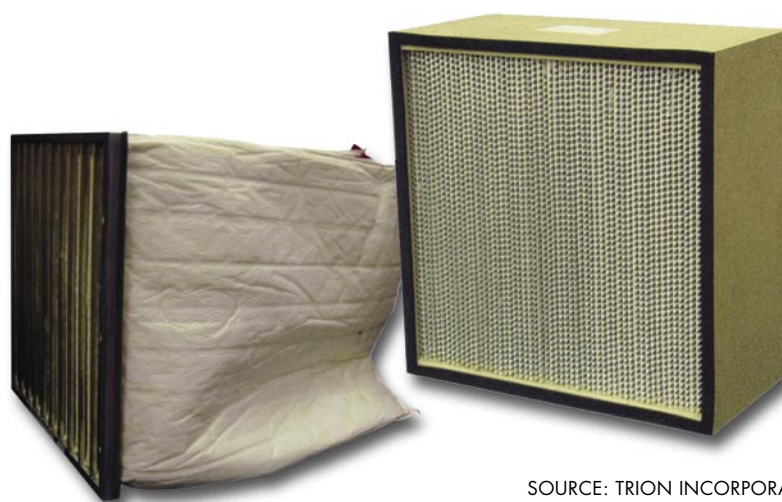
HEPA filters are typically rated as 99.97 percent effective in removing dust and particulate matter greater than 0.3 micron in size. The performance of high efficiency ASHRE filters is defined in terms of their total arrestance. Graphs of filter efficiency versus particle size do not constitute performance requirements and are merely a convenient way of describing performance (see Figure 5-6). Filters with the same total arrestance may have different performance curves.

Table 5-1: Comparison of ASHRAE Standards 52.1 and 52.2

ASHRAE 52.2				ASHRAE 52.1		Particle Size Range, μm	Applications
	Particle Size Range			Test			
MERV	3 to 10 μm	1 to 3 μm	0.3 to 1 μm	Arrestance	Dust Spot		
1	< 20%	-	-	< 65%	< 20%	> 10	Residential, light, pollen, dust mites
2	< 20%	-	-	65 - 70%	< 20%		
3	< 20%	-	-	70 - 75%	< 20%		
4	< 20%	-	-	> 75%	< 20%		
5	20 - 35%	-	-	80 - 85%	< 20%	3.0 - 10	Industrial, dust, molds, spores
6	35 - 50%	-	-	> 90%	< 20%		
7	50 - 70%	-	-	> 90%	20 - 25%		
8	> 70%	-	-	> 95%	25 - 30%		
9	> 85%	< 50%	-	> 95%	40 - 45%	1.0 – 3.0	Industrial, Legionella, dust
10	> 85%	50 - 65%	-	> 95%	50 - 55%		
11	> 85%	65 - 80%	-	> 98%	60 - 65%		
12	> 90%	> 80%	-	> 98%	70 - 75%		
13	> 90%	> 90%	< 75%	> 98%	80 - 90%	0.3 – 1.0	Hospitals, Smoke removal, bacteria
14	> 90%	> 90%	75 - 85%	> 98%	90 - 95%		
15	> 90%	> 90%	85 - 95%	> 98%	~95%		
16	> 95%	> 95%	> 95%	> 98%	> 95%		
17	-	-	≥ 99.97%	-	-	< 0.3	Clean rooms, Surgery, chem-bio, viruses
18	-	-	≥ 99.99%	-	-		
19	-	-	≥ 99.999%	-	-		
20	-	-	≥ 99.9999%	-	-		

Note: This table is adapted from American Society of Heating, Refrigerating, and Air-conditioning Engineers (ASHRAE) Standard 52.2: *Method of Testing General Ventilation Air-cleaning Devices for Removal Efficiency by Particle Size*, Atlanta, GA., 1999 and Spengler, J.D., Samet, J.M., and McCarthy, J.F., *Indoor air quality Handbook*, New York, NY: McGraw-Hill, 2000.

Figure 5-5  
A bag filter and HEPA filter



SOURCE: TRION INCORPORATED

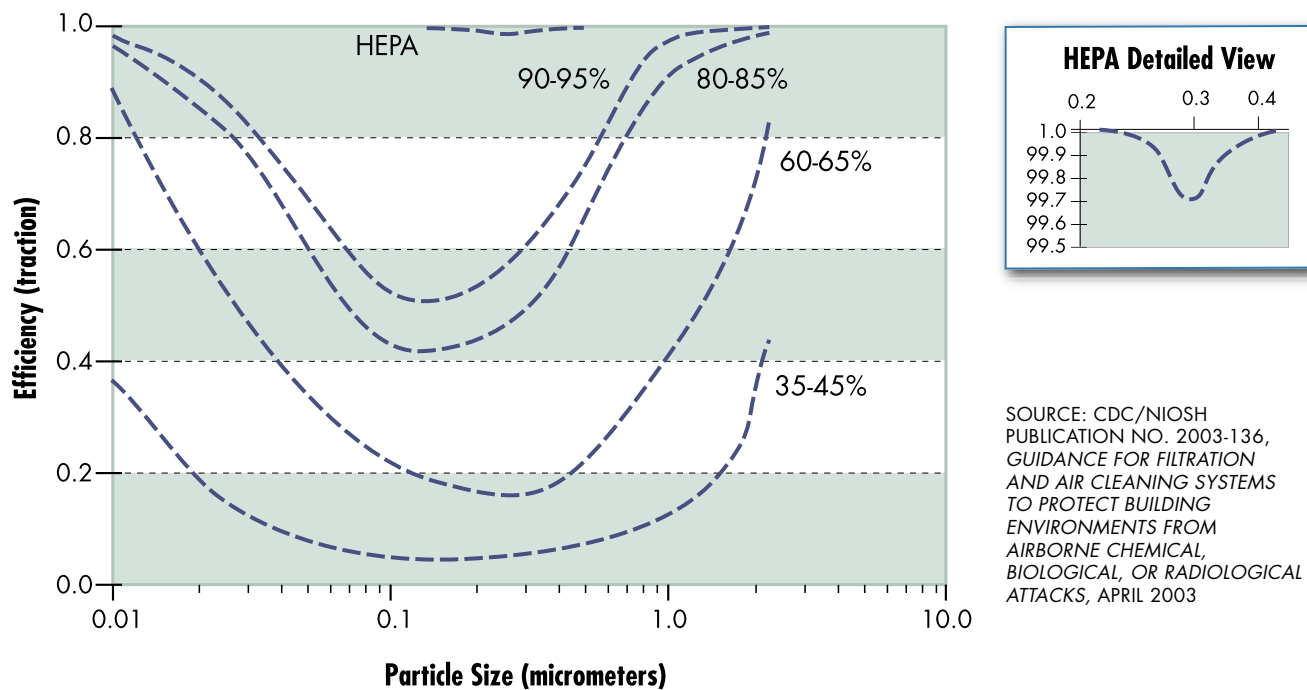


Figure 5-6 Comparison of filter collection efficiency based on particle size

Figure 5-7 is the characteristic performance curve of a typical HEPA filter with the design point indicated. The dip between 0.1 and 0.3 microns represents the most penetrating particle size. Many bacteria and viruses fall into this size range. Fortunately, microbes in this range are also vulnerable to ultraviolet radiation. For this reason, many health care facilities couple particulate air filters with ultraviolet germicidal irradiation (UVGI). UVGI will be discussed later in this section.

**Sorbent Filters.** Particulate filters are not intended to remove gases and vapors. Sorbent filters use one of two mechanisms for capturing and controlling gas-phase air contaminants, physical absorption or chemisorption.

Both mechanisms remove specific types of gas-phase contaminants in indoor air. Unlike particulate filters, sorbents cover a wide range of highly porous materials (see Figure 5-8), ranging from simple clays and carbons to complex engineered polymers. Many sorbents, with the exception of those that are chemically active, can be regenerated by application of heat or other processes.

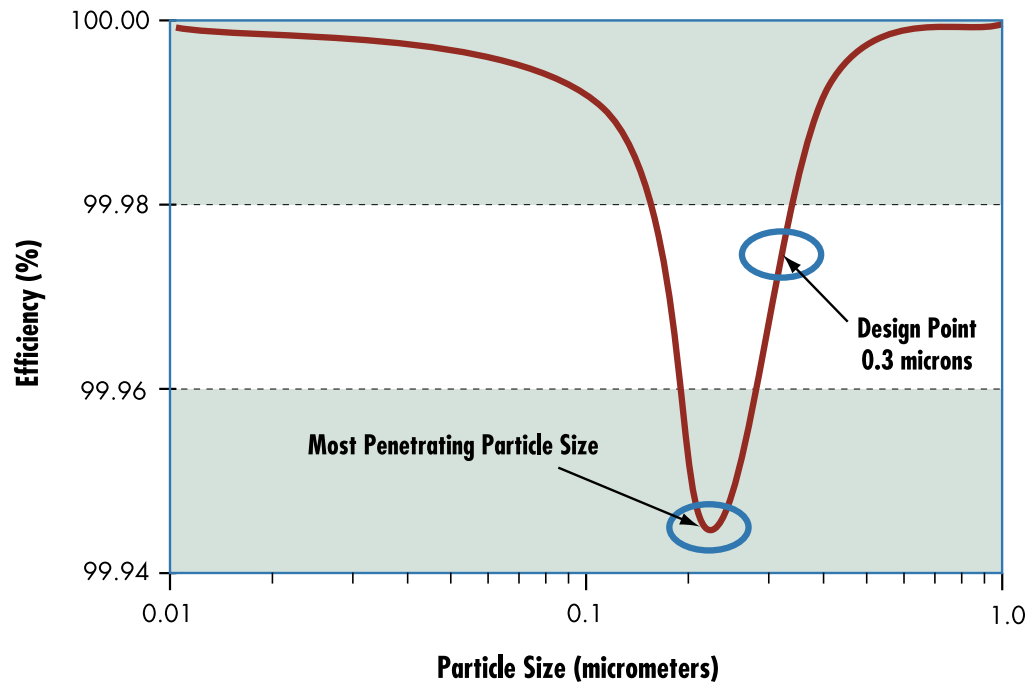


Figure 5-7 Typical performance of a HEPA 99.97%

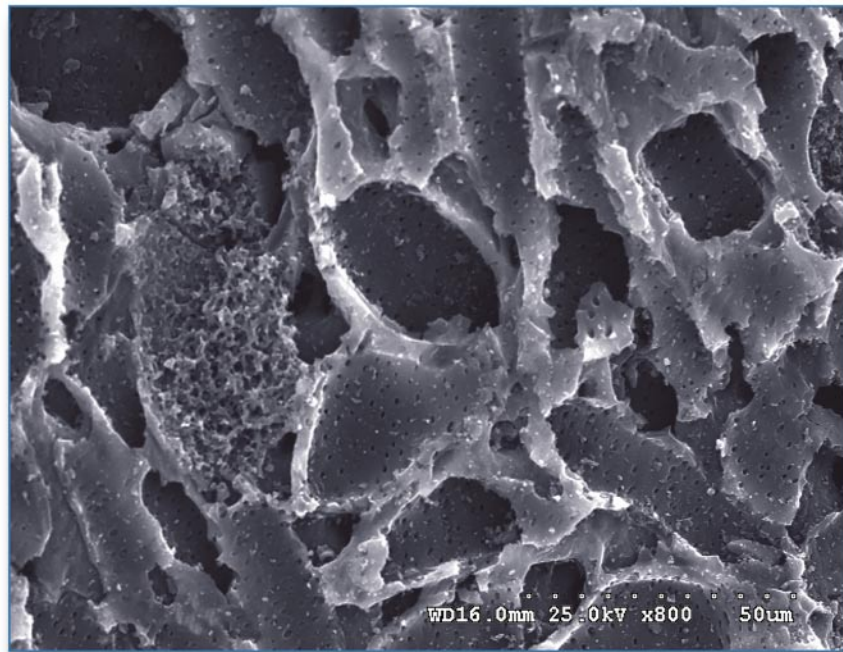


Figure 5-8 Scanning electron microscope image of activated carbon pores

SOURCE: CDC/NIOSH PUBLICATION NO. 2003-136, *GUIDANCE FOR FILTRATION AND AIR CLEANING SYSTEMS TO PROTECT BUILDING ENVIRONMENTS FROM AIRBORNE CHEMICAL, BIOLOGICAL, OR RADIOLOGICAL ATTACKS*, APRIL 2003

Understanding the precise removal mechanism for gases and vapors is often difficult due to the nature of the adsorbent and the processes involved. Although knowledge of adsorption equilibrium helps in understanding vapor protection, filter performance depends on such properties as mass transfer, chemical reaction rates, and chemical reaction capacity. Some of the most important parameters include the following:

- **Breakthrough concentration.** Breakthrough concentration is the downstream contaminant concentration, above which the sorbent is considered to be performing inadequately. Its concentration indicates the agent has broken through the sorbent, which is no longer providing maximum protection. This parameter is a function of loading history, relative humidity, and other factors.
- **Breakthrough time.** Breakthrough time is the elapsed time between initial contact of the toxic agent, at a reported challenge concentration, with the upstream surface of the sorbent bed and the time at which the breakthrough concentration occurs on the downstream side of the sorbent bed.
- **Challenge concentration.** Challenge concentration is the airborne concentration of the hazardous agent entering the sorbent.
- **Residence time.** Residence time is the length of time that the hazardous agent spends in contact with the sorbent. This term is generally used in the context of superficial residence time, which is calculated on the basis of the adsorbent bed volume and the volumetric flow rate.
- **Mass transfer zone or critical bed depth.** Mass transfer zone or critical bed depth are interchangeably used terms. They refer to the adsorbent bed depth required to reduce the chemical vapor challenge to the breakthrough concentration. When applied to the challenge chemicals that are removed by chemical reaction, mass transfer is not as precise a descriptor, but is often used in that context. The portion of the adsorbent bed not included in the mass transfer zone is often termed the capacity zone.

Choosing the appropriate sorbent or sorbents for an airborne contaminant is a complex decision that involves many factors. The installation of sorbent filters for the removal of gaseous contaminants from a building's air is a less common practice than the installation of particulate filtration. Sorbents have different affinities, removal efficiencies, and saturation points for each chemical agent. The EPA states that a well-designed adsorption system should have removal efficiencies ranging from 95 percent to 98 percent for industrial contaminant concentrations in the range of 500 to 2,000 ppm; higher collection efficiencies are needed for high toxicity CBR agents. Sorbent physicochemical properties (e.g., pore size and shape, surface area, pore volume, and chemical inertness) all influence the ability of a sorbent to collect gases and vapors. Sorbent manufacturers have published extensive information regarding the proper use of gas-phase sorbents, based upon contaminants and conditions. The air contaminant's concentration, molecular weight, molecule size, and temperature are all important.

Sorbents are rated in terms of adsorption capacity (i.e., the amount of the chemical that can be captured) for many chemicals. This capacity rises as concentration increases and temperature decreases. The rate of adsorption (i.e., the efficiency) falls as the amount of contaminant captured grows. Adsorption capacity information (available from manufacturers, scientific literature, and the Internet) allows users to predict the service life of a sorbent bed.

Gases are removed in the sorbent bed's mass transfer zone. As the sorbent bed removes gases and vapors, the leading edge of this zone is saturated with the contaminant, while the trailing edge is clean, as dictated by the adsorption capacity, exposure history, and filtration dynamics. Significant quantities of the air contaminant may pass through the sorbent bed if breakthrough occurs. Breakthrough may be avoided by selecting the appropriate quantity of sorbent and performing regular maintenance.

Activated carbon (see Figure 5-9) is the most common sorbent. The huge surface area of activated carbon gives it countless

bonding sites. Typically, the pores in highly activated carbon have a total surface area of over 1,000 square meters per gram. Common substances used as a base material for producing carbon are wood, coal, and coconut shell. Impregnating carbon with special chemicals can enhance the absorption of specific gases. A broad-based chemical addition typically used is copper-silver-zinc-molybdenum-triethylenediamine (ASZM-TEDA). Both the DOS and DoD currently recommend ASZM-TEDA sorbent for collecting classical chemical warfare agents.



Figure 5-9 Charcoal filter beds

SOURCE: FLANDERS CORPORATION

Sorbent filters should be located downstream of the particulate filters. This arrangement allows the sorbent to collect vapors generated from liquid aerosols collected on the particulate filter and reduces the amount of particulate reaching the sorbent. Gas-phase contaminant removal can potentially be a challenging and costly undertaking, and different factors should be addressed.

All sorbents have limited adsorption capacities and require scheduled maintenance. The effective residual capacity of an activated carbon sorbent bed is not easily determined while in use, and saturated sorbents can re-emit collected contaminants. Sorbent life depends upon bed volume or mass, along with shape, which influences airflow through the sorbent bed. Chemical agent concentrations and other gases (including humidity) affect the bed capacity. Because of differences in affinities, it is possible that one chemical may displace another chemical, which can be re-adsorbed downstream or forced out of the bed. Most sorbents come in pellet form, which makes it possible to mix them. Mixed- and/or layered-sorbent beds permit effective removal of a broader range of contaminants than possible with a single sorbent. Many sorbents can be regenerated, and it is important to closely follow manufacturers' guidance to ensure that sorbents are replaced or regenerated in a safe and effective manner.

Some chemically active sorbents are impregnated with strong oxidizers, such as potassium permanganate. The adsorbent part



of the bed captures the target gas and gives the oxidizer time to react and destroy other agents. Chemically active sorbents should not be reused because the oxidizer is consumed over time. If the adsorbent bed is exposed to high concentrations of vapors, exothermic adsorption could lead to a large temperature rise and filter bed ignition. This risk can be exacerbated by the nature of impregnation materials. It is well known that lead and other metals can significantly lower the spontaneous ignition temperature of a carbon filter bed. Sorbent bed fires are extremely dangerous, and steps should be taken to avoid this hazard. These systems should be located away from heat sources and automatic shut-off and warning capabilities should be included in the system.

**Air Filtration Considerations.** In addition to proper filter or sorbent selection, the following must be considered when installing or upgrading filtration systems:

- **Filter bypass** is a common problem found in many HVAC filtration systems. It occurs when air, rather than moving through the filter, goes around it, decreasing collection efficiency and defeating the intended purpose of the filtration system. Filter bypass is often caused by poorly fitting filters, poor sealing of filters in their framing systems, missing filter panels, or leaks and openings in the air handling unit downstream of the filter bank and upstream of the blower. Simply improving filter efficiency without addressing filter bypass provides little, if any, improvement to system efficiency.
- **Cost** is another issue affected by HVAC filtration systems. Both first and life-cycle costs should be considered (e.g., initial installation, replacement, operating, maintenance, etc.). Not only are higher-efficiency filters and sorbent filters more expensive than the filters traditionally used in HVAC systems, but fan units may also need to be upgraded to handle the increased pressure drop associated with the upgraded filtration systems. Although improved filtration will normally come at a higher cost, many of these costs can be partially offset by the beneficial effects, such as cleaner (and



more efficient) HVAC components and improved indoor environmental quality.

- **Filtration and air-cleaning** affect only the air that passes through the filtration and air-cleaning device, whether it is outdoor air, recirculated air, or a mixture of the two. Building envelopes in residential and commercial buildings are, in general, quite leaky, and significant quantities of air can infiltrate the building envelope with minimal filtration. Field studies have shown that, unless specific measures are taken to reduce infiltration, as much air may enter a building through infiltration as through the mechanical ventilation system. Therefore, building managers should not expect filtration alone to protect a building from outdoor releases, particularly for systems in which no make-up air or inadequate over-pressure is present. Instead, filtration in combination with other steps, such as building pressurization and tightening the building envelope, should be considered to increase the likelihood that the air entering the building actually passes through the filtration and air-cleaning systems.

**Ultraviolet Germicidal Irradiation (UVGI).** UVGI has long been used in laboratories and health care facilities. Ultraviolet radiation in the range of 2,250-3,020 Angstroms is lethal to microorganisms. All viruses and almost all bacteria (excluding spores) are vulnerable to moderate levels of UVGI exposure. Spores, which are larger and more resistant to UVGI than most bacteria, can be effectively removed through high efficiency air filtration. For these reasons, today most UVGI systems are installed in conjunction with high efficiency filtration systems in many health care facilities.

Ultraviolet (UV) lamps resemble ordinary fluorescent lamps (see Figure 5-10), but are specially designed to emit germicidal UV and include a glass envelope to filter out harmful, ozone forming radiation. The lamps are available in a variety of sizes and shapes and must be mounted in special housings and located so that people are not exposed to direct irradiation. Newer more advanced compact UV tubes provide higher output in the UV-C bandwidth



Figure 5-10  
UVGI array used for air disinfection with reflective surfaces

SOURCE: LUMALIER  
INCORPORATED

(253.7 nanometer wavelength) and increased reliability. UVGI safety measures, such as duct access interlocks that turn off the lamps when the duct housing is opened, should be used.

Manufacturers offer UVGI systems suitable for in-duct or large plenum installations. Retrofitting UVGI systems can also be relatively simple if sufficient space is available. There are UV lamps that can be mounted externally in ductwork and pressure losses across such lamps are often negligible. When installing a UVGI system, attention must be paid to maintaining design air velocity and temperature of the UV lamps. Cooling the plasma inside a UV lamp can significantly affect its UV output. Polished aluminum reflective panels can also be used to increase the intensity of a UVGI field in an enclosed duct or chamber. The design velocity for a typical UVGI unit is similar to that of particulate filters (about 400 feet per minute). It is very important to properly design and install UVGI systems in order to obtain the desired effects. Improper systems may provide a false sense of protection. For a discussion of the factors that should be considered when designing and sizing a UVGI system, additional information can be found in W. J. Kowalski, *Immune Building Systems Technology* (McGraw Hill, 2003).

A design utilizing a combination of filtration and UVGI can be very effective against biological agents. Smaller microbes, which are difficult to filter out, tend to be more susceptible to UVGI; while larger microbes, such as spores, which are more resistant to UVGI, tend to be easier to filter out.

#### **5.4.2 Applying External Filtration**

Applying external filtration to a building requires modifications to the building's HVAC system and electrical system, and it also usually requires minor architectural changes to reduce air leakage from the selected protective envelope. These changes are necessary to ensure that, when the protective system is in operation, all outside air enters the building through the filters. The air exchange that normally occurs due to wind, chimney effect, and operation of fans must be reduced to zero. This is

achieved mainly by introducing filtered air at a rate sufficient to produce an overpressure in the building and create an outward flow through all cracks, pores, seams, and other openings in the building envelope. For standby systems, dampers are normally required to tighten the envelope in transitioning to the protective mode. The level of overpressure required varies with weather conditions and height of the building.

The capacity of filtration units needed for protection is determined by the leakage characteristics and size of the building. The cost of installing a high efficiency filtration system varies directly with the leakage rate; higher leakage rate equals higher costs, and the need for additional heating and cooling capacity for the filtered air.

Filtration system capacity must be matched to the leakage of the building to achieve maximum protection. Fan-pressurization tests are usually performed on buildings to determine their normalized leakage rates. Nominal data on the leakage rates of various types of buildings are available in the U.S. Army Corps of Engineers Engineering Technical Letter (ETL) 1110-3-498, *Design of Collective Protection Shelters to Resist Chemical, Biological, and Radiological (CBR) Agents*, (February 24, 1999) and can be used to estimate the leakage rate of a building.

For a terrorist threat, the U.S. Army Corps of Engineers recommends a minimum HVAC CBR filtration system overpressure goal of 5 Pa (0.02 inch water gauge [wg]). This overpressure corresponds to an impact pressure normal to a wall from a 12-km/hr (7-mph) wind. After installation of an overpressure system (see Figure 5-11), it is possible that a pressure greater than 5 Pa (0.02 inch wg) will be achieved. A higher pressure provides a higher factor of safety and should not be intentionally lowered.



Figure 5-11  
A military FFA 580 air filtration system containing both a HEPA filter and an ASZM-TEDA carbon adsorber as part of an overpressure system

Currently, there are no criteria or guidance for the performance of filtration systems designed for protecting building occupants against CBR agents. The U.S. military has issued very conservative criteria in the ETL referenced above, which is not based on analytical or empirical research. Recent research in the field suggests significant levels of protection can be achieved with medium to high efficiency filters (see Figure 5-12), especially when used in combination with UVGI.<sup>1</sup> In a recent simulation in the Architectural Engineering Department of Pennsylvania State University, various combinations of MERV and UVGI Rating Values (URV) systems were modeled for a 20-story building subject to releases of anthrax, smallpox, and botulinum. No significant benefits were shown for filtration/URV levels beyond MERV 13/URV 13.<sup>2</sup>

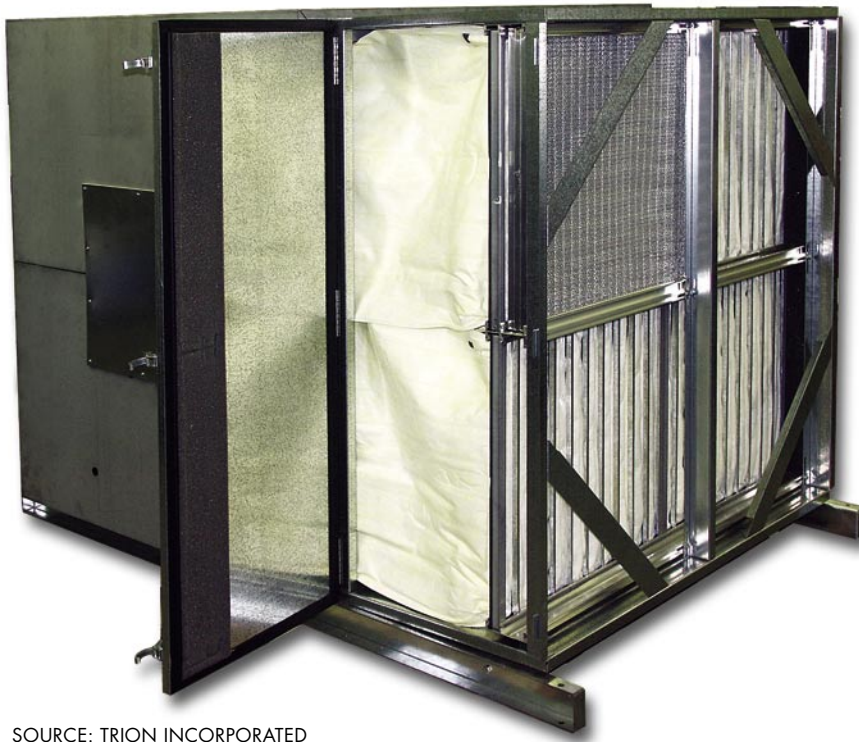


Figure 5-12  
A commercial air filtration unit

SOURCE: TRION INCORPORATED

<sup>1</sup> W. J. Kowalski, W. P. Bahnfleth, and T. S. Whittam, *Filtration of Airborne Microorganisms: Modeling and Prediction* <http://www.engr.psu.edu/ae/wjk/fom.html>.

<sup>2</sup> W. J. Kowalski, *Defending Buildings Against Bioterrorism, Engineering Systems*, September 30, 2002 [http://www.esmagazine.com/CDA/ArticleInformation/features/BNP\\_Features\\_Item/0,2503,84858,00.html](http://www.esmagazine.com/CDA/ArticleInformation/features/BNP_Features_Item/0,2503,84858,00.html).

Various types of high efficiency filter systems, both commercial and military, have been used for building protection. The current DoD recommended carbon for filtering a broad range of toxic chemical vapors and gases is ASZM-TEDA carbon per military specification EA-C-1704A maintained by the U.S. Army Edgewood Chemical Biological Center, Aberdeen Proving Ground, MD.

High efficiency air filtration can be most economically applied by integrating it into the HVAC system in the design of new construction. Application of filtration systems in retrofit involves greater costs.

Filter systems can be applied to protect either all or part of a building. At least part of the building is always excluded from the envelope being protected (i.e., areas having or requiring high rates of air exchange with the outdoors, such as mechanical rooms containing boilers or generators and receiving areas). Mechanical rooms that contain air handling units must be included within the protective envelope. Filter systems may be designed to operate on either a continuous duty cycle or on standby. The assumption with the latter is that they will be turned on when there is greater likelihood of an airborne hazard occurring.

The disadvantage of external air filtration is its high costs for hardware, installation, operation, and maintenance. The main cost component of operating the filter units is the electrical power required to force air through the filters. The airflow resistance of HEPA filters is typically about 1 inch wg, and this resistance increases steadily as the filter loads with dust or other fine particles in service. For high efficiency carbon filters, the pressure drop may range from about 1 to 4 inch wg. Maintenance costs involve periodic filter replacement. Particulate filter change-out is generally based on the airflow resistance rising to unacceptable levels.

There is no simple means for determining how much capacity remains in a carbon filter. Because the service life varies with the environment in which it operates, it can be replaced according

to time in service using a conservative estimate, or its remaining capacity can be measured by the use of test canisters. With the reserve capacity normally designed into carbon filters, a filter can maintain efficiency greater than 99.999 percent for about 3 years of continuous use with ASZM-TEDA carbon, depending upon the quality of air in the environment it operates.

### **5.4.3 Applying Internal Filtration (Recirculation Filter Units)**

Internal filtration can be applied much more easily, in many cases without any modifications to the building or installation costs; however, it provides a much lower level of protection against an external release than does high efficiency external filtration. One advantage of internal filtration is in purging contaminants from a building following an internal release. Also referred to as recirculation filtering, the protection it provides against an external release is dependent upon the rate at which air in the building envelope is exchanged with outdoor air. The tighter the building, the greater the protection achieved with internal filtration.

Recirculation filter units can be employed to increase protection achieved by sheltering in place. This involves the use of free-standing units referred to as indoor air purifiers or indoor air quality filter units. Many of these contain filters for removal of both aerosols and chemicals vapors. These typically have high efficiency filters for the removing aerosols (HEPA filters); however, the chemical filters are of relatively low efficiency, typically ranging from less than 50 percent to as high as 99 percent. Because of the relatively high efficiency of the HEPA filter versus the carbon filter, typically available in recirculation filter units, these units can provide a higher level of protection against an aerosol than against chemical vapors. The carbon filters also do not typically contain the impregnated carbon capable of removing chemicals of high vapor pressure. Manufacturers provide guidance on the size of room a single unit will accommodate. Because these filters are designed mainly for filtering pollen and dust and removing odors, there are no claims or guidance as to their protective capability.



Internal filtration can also be applied by simply installing higher efficiency particulate filters and/or carbon filters in place of standard dust filters in air handling units. Air handling units are not designed, however, to accommodate the large increase in airflow resistance a high efficiency filter or carbon filter would add. The capability of the existing air handling unit must be examined before such installations are attempted. In typical air handling units, dust filter slots allow relatively high bypass around the filter media, reducing overall efficiency of the HEPA filters. Internal filtration protection against biological agents can also be enhanced through the installation of an UVGI system as discussed earlier.

#### **5.4.4 Radiological Hazards**

Radiological hazards can be divided into three general forms: alpha, beta, and gamma radiation, which are emitted by radioisotopes that may occur as an aerosol, be carried on particulate matter, or occur in a gaseous state. Alpha particles, consisting of two neutrons and two protons, are the least penetrating and the most ionizing form of radiation. They are emitted from the nucleus of radioactive atoms and transfer their energy at very short distances. Alpha particles are readily shielded by paper or skin and are most dangerous when inhaled and deposited in the respiratory tract. Beta particles are negatively charged particles emitted from the nucleus of radioactive atoms. Beta particles are more penetrating than alpha particles, presenting an internal exposure hazard. They can penetrate the skin and cause burns. If they contact a high density material, they may generate x-rays also known as “Bremmstrahlung radiation.” Gamma particles are emitted from the nucleus of an atom during radioactive decay. Gamma radiation can cause ionization in materials and biological damage to human tissues, presenting an external radiation hazard.

There are three primary scenarios in which radioactive materials could be dispersed by a terrorist: use of conventional explosives or other means to spread radioactive materials (a dirty bomb), attack on a fixed nuclear facility, and use of a nuclear weapon. In any of these events, filtration and air cleaning devices would be ineffec-

tive at stopping the radiation itself; however, they would be useful in collecting the material from which the radiation is emitted. Micrometer-sized aerosols from a radiological event are effectively removed from air streams by HEPA filters. This collection could prevent distribution throughout a building; however, decontamination of the HVAC system would be required.

## **5.5 EXHAUSTING AND PURGING**

Turning on building ventilation fans and smoke-purge fans is a protective action for purging airborne hazards from the building and reducing occupant exposure, but it is mainly useful when the source of the hazard is indoors.

Purging must be carefully applied with regard to the location of the source and the time of the release. It must be clear that the source of the hazard is inside the building and, if not, purging should not be attempted. If the hazardous material has been identified before release or immediately upon release, purging should not be employed, because it may spread the hazardous material throughout the building or HVAC zone. In this case, all air handling units should be turned off to isolate the hazard while evacuating or temporarily sheltering in place.

Additionally, the ventilation system and smoke purge fans can be used to purge the building following an external release after the hazard outdoors has dissipated, and it has been confirmed that the agent is no longer present near the building.

## **5.6 CBR DETECTION**

Most strategies for protecting people from airborne hazards require a means of detection (i.e., determining that a hazard exists). Although effective and inexpensive devices are widely available to detect, for example, smoke and carbon monoxide, there are no detectors that can rapidly alert occupants to a broad range of chemical and biological hazards.



Chemical detection technology has improved vastly since Operation Desert Storm, where many military detection systems experienced high false alarm rates, but biological detection technology has not matured as fast. Biological signatures are not as distinctive as chemical signatures and can take 30 minutes or more to detect. Biological detection systems are expensive and generally require trained specialists to operate. Current chemical detectors work in approximately 10 seconds; however, the current state of biological and chemical detection is limited to detecting specific agents. There currently is no all-inclusive detection system available. Wide varieties of efficient radiological detectors have been developed for the nuclear industry and are commercially available. The NBC Products and Services Handbook, which was discussed in Section 5.3, contains a catalogue of CBR detection equipment. Additionally, the NIJ has reviewed chemical and biological detection devices in NIJ Guide 100-00: *Guide for the selection of Chemical Agent and Toxic Industrial Material Detection Equipment for Emergency First Responders*, June 2000; and NIJ Guide 101-00: *An Introduction to Biological Agent Detection Equipment for Emergency First Responders*, December 2001.

**Chemical Detectors.** Driven largely by a desire to protect workers from toxic vapors in industrial environments, considerable information is known on the toxicity of chemical warfare agents, which often have dual uses in industry. A variety of detection technologies exist, ranging from inexpensive manual point detection devices (e.g., paper strips and calorimetric tubes) utilizing basic chemical reactions to trigger color changes, to sophisticated detection systems utilizing advanced technologies.

Chemical agents do not possess universal properties that permit detection by any single method. Therefore, most chemical detectors are designed to detect specific agents or a group of related agents. Most broad range detection systems actually combine several different sensors utilizing different technologies and can be very expensive and complex. Nevertheless, today there are numerous commercially available chemical detectors. The most capable detectors utilize ion mobility spectrometry (IMS), surface

acoustic wave (SAW), or gas chromatograph/mass spectrometer (GC/MS) technologies to detect chemical agents and toxic industrial materials (TIMs).

IMS detectors draw gaseous samples with an air pump into a reaction chamber where a radioactive source ionizes the sample. The ionized sample is then injected into a closed drift tube through a shutter that isolates the sample from atmospheric air. The drift tube has a weak electric field that draws the sample toward an ion detector. An electrical charge is generated upon impact with the ion detector. The time it takes for species to traverse the field and the intensity of the charge generated are used as a means of identifying the chemical agent.

SAW detectors consist of piezoelectric crystals coated with a film specially designed to absorb chemical agents from the air. They typically use multiple piezoelectric crystals coated with different polymeric films, each designed to absorb a particular class of volatile compound. The piezoelectric crystals absorb chemical vapors, which cause the resonant frequency of the crystal to change. By monitoring the resonant frequency of the different piezoelectric crystals, a response pattern of the system for a particular vapor is generated. Many SAW devices use pre-concentration tubes to reduce environmental interferences and increase detector sensitivity.

A GC uses inert gas to transport a sample of air through a long chromatographic column. Each molecule sticks to the column with a different amount of force and does not travel down the column at the same speed as the carrier gas. This causes the chemical agents and interferants to come out of the end of the column at different times (called the retention time). Because the retention time is known for the chemical agents, the signal from an associated detector is only observed for a short period starting before and ending just after the retention time of the chemical agent, eliminating false alarms from similar compounds that have different retention times. Using a pre-concentrator specific to the analyte can also reduce false alarms caused by interferants.

Mass spectrometry is a technique that can positively identify a chemical agent at very low concentrations. In this technique, a volatilized sample is ionized, typically by an electron beam, which also causes the molecule to fragment into smaller ionized pieces. The ionized molecules and fragments are then passed into a mass analyzer that uses electric fields to separate the ions according to the ratio of their mass divided by their electric charge. The analyzer allows only ions of the same mass over charge ratio to impinge upon the detector. By scanning the electric potentials in the mass analyzer, all the different mass/charge ions can be detected. The result is a mass spectrum that shows the relative amount and the mass of each fragment, and the unfragmented parent molecule. Because each molecule forms a unique set of fragments, mass spectroscopy provides positive identification. To simplify interpretation of the mass spectrum, it is best to introduce only one compound at a time. This is often achieved by using a gas chromatograph to separate the components in the sample. The end of the gas chromatography column is connected directly to the inlet of the mass spectrometer. When used in combination, a GC/MS is one of the most sensitive and discerning tools for identifying chemical and biological compounds; however, it requires significant skill to operate and interpret the results.

Today, there are commercially available IMS detection systems that will detect most chemical agents and many TIMs (see Figure 5-13). They are suitable for integration into a building's HVAC system, can interface with HVAC control systems, have reasonable maintenance requirements (every 3 months), low false alarm rates, and can be programmed to detect specific chemical agents.

**Biological Detectors.** The current state of biological detection technology is very different from that of chemical agent detection technology. In general, most biological detection systems are currently in the research and early development stages. There are some commercially available devices that have limited utility (responding only to a small number of agents) and are generally



Figure 5-13  
An IMS chemical detector  
designed for installation in  
HVAC systems

SOURCE: SMITHS DETECTION

high cost items. Because commercially available biological warfare (BW) detection systems and/or components exhibit limited utility in detecting and identifying BW agents and are also costly, it is strongly recommended that purchasers be very careful when considering any device that claims to detect BW agents.

One reason for the lack of available biological detection equipment is that detection of biological agents requires extremely high sensitivity (because of the very low effective dose needed to cause infection and spread the disease) and an unusually high degree of selectivity (because of the large and diverse biological background in the environment). Another reason for the lack of biological detection equipment is that biological agents, compared to chemical agents, are very complex systems of molecules, which makes them much more difficult to identify. For example, ionization/ion mobility spectrometry, an excellent system for collection, detection, and identification of chemical agents, cannot detect or discriminate biological agents in their current forms. In fact, the need for high efficiency collection and concentration of the sample, high sensitivities, and high selectivities make almost all chemical detectors in their current form unusable for biological agent detection.

Because of the need for high selectivity and sensitivity, biological detection systems are necessarily complex and expensive devices. In general, biological sensors can detect one specific agent, and can usually only be used once. Some biological sensors are in current use in the food industry. The U.S. military is developing several detection systems that show some promise. However, these systems are very complicated, require highly trained operators, extensive maintenance, and are extremely expensive to purchase and operate.

For all these reasons, biological detection technologies will not be discussed herein. One alternative could be to use particle detectors. In theory, biological agents could be identified by a particle detector based on their characteristic size range. In fact, most biological detectors use trigger or cue technology to identify a change in the particulate background at the sensor to trigger the additional components of the detection system into

operation. However, in practice, there are numerous problems when attempting to identify biological agents with particle detectors. Particulates in the atmosphere originate from a number of sources. Dust, dirt, pollen, and fog are all examples of naturally occurring particulates found in the air. Manmade particulates such as engine exhaust, smoke, and industrial effluents (smokestacks) also contribute significantly to the environmental particulate background. The particulate background can change on a minute-by-minute basis, depending on the meteorological conditions at the time. For example, the particulate background next to a road will change dramatically, depending on whether there is traffic on the road disturbing the dust, or if the road is empty. Likewise, if there is little wind, not many particulates are carried into the atmosphere; however, when the wind begins to blow, it can carry many particulates from the immediate vicinity, as well as from remote locations. The challenge for a biological detection system is to be able to discriminate between all of the naturally occurring particulates and the biological agent particulates. Thus, identification of biological agents with particle detectors alone may be extremely difficult.

## **5.7 INDICATIONS OF CBR CONTAMINATION**

Most hazardous chemicals have warning properties that provide a practical means for detecting a hazard and initiating protective actions. Such warning properties make chemicals perceptible; for example, vapors or gases can be perceived by the human senses (i.e., smell, sight, taste, or irritation of the eyes, skin, or respiratory tract) before serious effects occur. The distinction between perceptible and imperceptible agents is not an exact one. The concentrations at which a person can detect an odor vary from person to person, and these thresholds also vary relative to the concentration that can produce immediate, injurious effects.

Most of the industrial chemicals and chemical-warfare agents are readily detectable by smell. Soldiers in World Wars I and II were taught to identify, by smell, such agents as mustard, phosgene, and chlorine, and this detection method proved effective for

determining when to put on and take off a gas mask. An exception is the chemical-warfare agent sarin, which is odorless and colorless in its pure form and, therefore, imperceptible. Among the most common toxic industrial chemicals, carbon monoxide is one of the few that is imperceptible.

Biological agents are also imperceptible and there are no detection devices that can determine their presence in the air in real time. Current methods for detecting bacterial spores, such as anthrax, require a trained operator and expensive equipment. It is not currently possible to base protective responses to biological agents on detection.

Researchers are working on a prototype device to automatically and continuously monitor the air for the presence of bacterial spores. The device would continuously sample the air and use microwaves to trigger a chemical reaction, the intensity of which would correspond to the concentration of bacterial spores in the sample. If an increase in spore concentration is detected, an alarm similar to a smoke detector would sound and a technician would respond and use traditional sampling and analysis to confirm the presence of anthrax spores. Researchers hope the device response time will be fast enough to help prevent widespread contamination.

In the absence of a warning property, people can be alerted to some airborne hazards by observing symptoms or effects in others. This provides a practical means for initiating protective actions, because the susceptibility to hazardous materials varies from person to person. The concentrations of airborne materials may also vary substantially within a given building or room, producing a hazard that may be greater to some occupants than to others.

Other warning signs of a hazard may involve seeing and hearing something out of the ordinary, such as the hiss of a rapid release from a pressurized cylinder. Awareness to warning properties, signs, and symptoms in other people is the basis of a protective action plan. Such a plan should apply four possible protective actions: sheltering in place, using protective masks, evacuating, and purging, as already discussed in this chapter.

For protection against imperceptible agents, the only practical protective measures are those that are continuously in place, such as filtering all air brought into the building on a continuous basis and using automatic, real-time sensors that are capable of detecting the imperceptible agents.

Chemical, biological, and radiological materials, as well as industrial agents, may travel in the air as a gas or on surfaces we physically contact. Dispersion methods may be as simple as placing a container in a heavily used area, opening a container, or using conventional (garden)/commercial spray devices, or as elaborate as detonating an aerosol.

Chemical incidents are characterized by the rapid onset (minutes to hours) of medical symptoms and easily observed indicators (e.g., colored residue, dead foliage, pungent odor, and dead animals, birds, fish, or insects; see Table 5-2 and Figure 5-14).

In the case of a biological incident, the onset of symptoms takes days to weeks and, typically, there will be no characteristic indicators (see Table 5-3 and Figure 5-15). Because of the delayed onset of symptoms in a biological incident, the area affected may be greater due to the migration of infected individuals.

In the case of a radiological incident, the onset of symptoms also takes days to weeks to occur and typically there will be no characteristic indicators (see Table 5-4 and Figure 5-16). Radiological materials are not recognizable by the senses because they are colorless and odorless.

Specialized equipment is required to determine the size of the affected area and if the level of radioactivity presents an immediate or long-term health hazard. Because of the delayed onset of symptoms in a radiological incident, the affected area may be greater due to the migration of contaminated individuals.

Table 5-2: Indicators of a Possible Chemical Incident

<b>Dead animals, birds, fish</b>	Not just an occasional roadkill, but numerous animals (wild and domestic, small and large), birds, and fish in the same area.
<b>Lack of insect life</b>	If normal insect activity (ground, air, and/or water) is missing, check the ground/water surface/shore line for dead insects. If near water, check for dead fish/aquatic birds.
<b>Physical symptoms</b>	Numerous individuals experiencing unexplained water-like blisters, wheals (like bee stings), pinpointed pupils, choking, respiratory ailments, and/or rashes.
<b>Mass casualties</b>	Numerous individuals exhibiting unexplained serious health problems ranging from nausea to disorientation to difficulty in breathing to convulsions to death.
<b>Definite pattern of casualties</b>	Casualties distributed in a pattern that may be associated with possible agent dissemination methods.
<b>Illness associated with confined geographic area</b>	Lower attack rates for people working indoors than those working outdoors, and vice versa.
<b>Unusual liquid droplets</b>	Numerous surfaces exhibit oily droplets/film; numerous water surfaces have an oily film. (No recent rain.)
<b>Areas that look different in appearance</b>	Not just a patch of dead weeds, but trees, shrubs, bushes, food crops, and/or lawns that are dead, discolored, or withered. (No current drought.)
<b>Unexplained odors</b>	<b>Smells may range from fruity to flowery to sharp/pungent to garlic/horseradish-like to bitter almonds/peach kernels to new mown hay. It is important to note that the particular odor is completely out of character with its surroundings.</b>
<b>Low-lying clouds</b>	Low-lying cloud/fog-like condition that is not explained by its surroundings.
<b>Unusual metal debris</b>	Unexplained bomb/munitions-like material, especially if it contains a liquid. (No recent rain.)



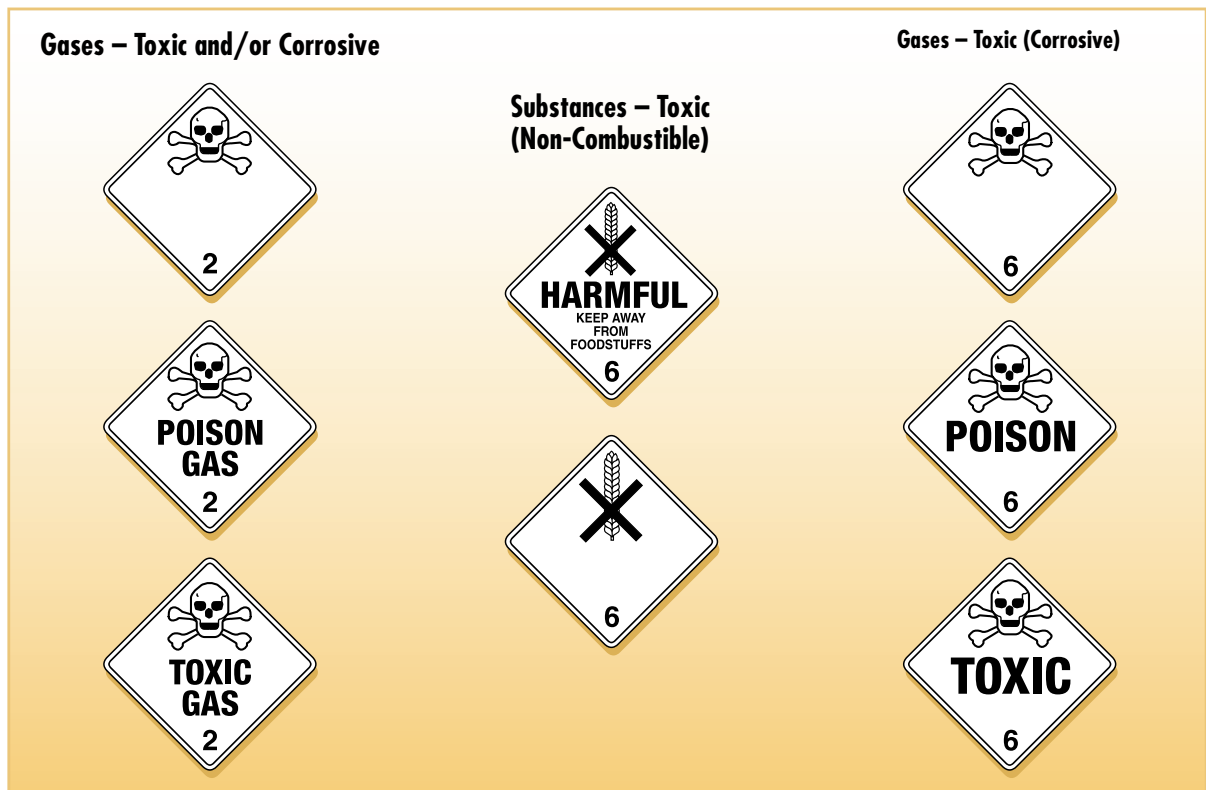


Figure 5-14 Placards associated with chemical incidents

Table 5-3: Indicators of a Possible Biological Incident

<b>Unusual numbers of sick or dying people or animals</b>	Any number of symptoms may occur. As a first responder, strong consideration should be given to calling local hospitals to see if additional casualties with similar symptoms have been observed. Casualties may occur hours to days or weeks after an incident has occurred. The time required before symptoms are observed is dependent on the biological agent used and the dose received. Additional symptoms likely to occur include unexplained gastrointestinal illnesses and upper respiratory problems similar to flu/colds.
<b>Unscheduled and unusual spray being disseminated</b>	Especially if outdoors during periods of darkness.
<b>Abandoned spray devices</b>	Devices will have no distinct odors.



Figure 5-15 Placards associated with biological incidents

Table 5-4: Indicators of a Possible Radiological Incident

<b>Unusual numbers of sick or dying people or animals</b>	As a first responder, strong consideration should be given to calling local hospitals to see if additional casualties with similar symptoms have been observed. Casualties may occur hours to days or weeks after an incident has occurred. The time required before symptoms are observed is dependent on the radioactive material used and the dose received. Additional symptoms likely to occur include skin reddening and, in severe cases, vomiting.
<b>Unusual metal debris</b>	Unexplained bomb/munitions-like material.
<b>Radiation symbols</b>	Containers may display a radiation symbol.
<b>Heat emitting material</b>	Material that seems to emit heat without any sign of an external heating source.
<b>Glowing material/particles</b>	If the material is strongly radioactive, it may emit a radioluminescence.



Figure 5-16 Placards associated with radiological incidents

This appendix contains some acronyms that do not actually appear in this manual. They have been included to present a comprehensive list that pertains to this series of publications.

## A

<b>AA&amp;E</b>	Arms, Ammunition, and Explosives
<b>AAR</b>	After Action Report
<b>ACL</b>	Access Control List
<b>ACP</b>	access control point
<b>ACS</b>	Access Control System
<b>ADA</b>	Americans with Disabilities Act
<b>ADAAG</b>	Americans with Disabilities Act Accessibility Guidelines
<b>AECS</b>	Automated Entry Control System
<b>AFJMAN</b>	Air Force Joint Manual, also may be known as AFMAN (I) for Air Force Manual
<b>AFMAN</b>	Air Force Manual
<b>ALERT</b>	Automated Local Evaluation in Real Time
<b>AMS</b>	Aerial Measuring System
<b>ANS</b>	Alert and Notification System
<b>ANSI</b>	American National Standards Institute
<b>ANSIR</b>	Awareness of National Security Issues and Response Program
<b>AOR</b>	Area of Responsibility

<b>AP</b>	armor piercing
<b>APHL</b>	Agency for Public Health Laboratories
<b>ARAC</b>	Atmospheric Release Advisory Capability
<b>ARC</b>	American Red Cross
<b>ARG</b>	Accident Response Group
<b>ARS</b>	Agriculture Research Service
<b>ASCE</b>	American Society of Civil Engineers
<b>ASHRAE</b>	American Society of Heating, Refrigerating, and Air-Conditioning Engineers
<b>ASTHO</b>	Association for State and Territorial Health Officials
<b>ASTM</b>	American Society for Testing and Materials
<b>ASZM-TEDA</b>	copper-silver-zinc-molybdenum-triethylenediamine
<b>AT</b>	Antiterrorism
<b>ATC</b>	Air Traffic Control
<b>ATF</b>	Bureau of Alcohol, Tobacco, and Firearms
<b>ATSD(CS)</b>	Assistant to the Secretary of Defense for Civil Support
<b>ATSDR</b>	Agency for Toxic Substances and Disease Registry
<b>AWG</b>	American wire gauge

## B

<b>BCA</b>	Benefit/Cost Analysis
<b>BCC</b>	Backup Control Center
<b>BCP</b>	Business Continuity Plan
<b>BDC</b>	Bomb Data Center

<b>BLASTOP</b>	Blast-Resistant Window Program
<b>BMS</b>	balanced magnetic switch
<b>BW</b>	biological warfare



<b>CAMEO</b>	Computer-Aided Management of Emergency Operations
<b>CB</b>	Citizens Band
<b>CBIAC</b>	Chemical and Biological Defense Information and Analysis Center
<b>CBR</b>	chemical, biological, or radiological
<b>CBRNE</b>	chemical, biological, radiological, nuclear, or explosive
<b>CCTV</b>	closed circuit television
<b>CDC</b>	Centers for Disease Control and Prevention
<b>CDR</b>	Call Detail Report
<b>CDRG</b>	Catastrophic Disaster Response Group
<b>CEO</b>	Chief Executive Officer
<b>CEPPO</b>	Chemical Emergency Preparedness and Prevention Office
<b>CERCLA</b>	Comprehensive Environmental Response, Compensation, and Liability Act
<b>CERT</b>	Community Emergency Response Team
<b>CFD</b>	Computational Fluid Dynamics
<b>CFO</b>	Chief Financial Officer
<b>CFR</b>	Code of Federal Regulations

<b>CHEMTREC</b>	Chemical Manufacturers' Association Chemical Transportation Emergency Center
<b>CHPPM</b>	Center for Health Promotion and Preventive Medicine
<b>CIAO</b>	Chief Infrastructure Assurance Office
<b>CIAO</b>	Critical Infrastructure Assurance Officer
<b>CICG</b>	Critical Infrastructure Coordination Group
<b>CIO</b>	Chief Information Officer
<b>CIP</b>	Critical Infrastructure Protection
<b>CIRG</b>	Crisis Incident Response Group
<b>CJCS</b>	Chairman of the Joint Chiefs of Staff
<b>CM</b>	Consequence Management
<b>CM</b>	Crisis Management
<b>CMS</b>	Call Management System
<b>CMU</b>	concrete masonry unit
<b>CMU</b>	Crisis Management Unit (CIRG)
<b>COB</b>	Continuity of Business
<b>COBIT™</b>	Control Objectives for Information Technology
<b>CO/DO</b>	Central Office/Direct Outdial
<b>CONEX</b>	Container Express
<b>CONOPS</b>	Concept of Operations
<b>COO</b>	Chief Operating Officer
<b>COOP</b>	Continuity of Operations Plan
<b>COR</b>	Class of Restriction
<b>COS</b>	Class of Service
<b>CPG</b>	Civil Preparedness Guide

<b>CPTED</b>	Crime Prevention Through Environmental Design
<b>CPX</b>	Command Post Exercise
<b>CRU</b>	Crisis Response Unit
<b>CSEPP</b>	Chemical Stockpile Emergency Preparedness Program
<b>CSI</b>	Construction Specifications Institute
<b>CSREES</b>	Cooperative State Research, Education, and Extension Service
<b>CST</b>	Civil Support Team
<b>CSTE</b>	Council of State and Territorial Epidemiologists
<b>CT</b>	Counterterrorism
<b>CW/CBD</b>	Chemical Warfare/Contraband Detection

## D

<b>DBMS</b>	Database Management System
<b>DBT</b>	Design Basis Threat
<b>DBU</b>	dial backup
<b>DD</b>	Data Dictionary
<b>DES</b>	Data Encryption Standard
<b>DEST</b>	Domestic Emergency Support Team
<b>DFO</b>	Disaster Field Office
<b>DHS</b>	Department of Homeland Security
<b>DISA</b>	Direct Inward System Access
<b>DMA</b>	Disaster Mitigation Act of 2000
<b>DMAT</b>	Disaster Medical Assistance Team

<b>DMCR</b>	Disaster Management Central Resource
<b>DMORT</b>	Disaster Mortuary Operational Response Team
<b>DOC</b>	Department of Commerce
<b>DoD</b>	Department of Defense
<b>DOE</b>	Department of Energy
<b>DOJ</b>	Department of Justice
<b>DOS</b>	Department of State
<b>DOT</b>	Department of Transportation
<b>DPP</b>	Domestic Preparedness Program
<b>DRC</b>	Disaster Recovery Center
<b>DTCTPS</b>	Domestic Terrorism/Counterterrorism Planning Section (FBI HQ)
<b>DTIC</b>	Defense Technical Information Center
<b>DTM</b>	data-transmission media
<b>DWI</b>	Disaster Welfare Information

## E

<b>EAS</b>	Emergency Alert System
<b>ECL</b>	Emergency Classification Level
<b>EECS</b>	Electronic Entry Control System
<b>EFR</b>	Emergency First Responder
<b>EM</b>	Emergency Management
<b>EMAC</b>	Emergency Medical Assistance Compact
<b>EMI</b>	Emergency Management Institute
<b>EMP</b>	electromagnetic pulse



<b>EMS</b>	Emergency Medical Services
<b>EOC</b>	Emergency Operations Center
<b>EOD</b>	Explosive Ordnance Disposal
<b>EOP</b>	Emergency Operating Plan
<b>EOP</b>	Emergency Operations Plan
<b>EPA</b>	Environmental Protection Agency
<b>EPCRA</b>	Emergency Planning and Community Right-to-Know Act
<b>EPG</b>	Emergency Planning Guide
<b>EPI</b>	Emergency Public Information
<b>EP&amp;R</b>	Directorate of Emergency Preparedness and Response (DHS)
<b>EPZ</b>	Emergency Planning Zone
<b>ERP</b>	Emergency Response Plan
<b>ERT</b>	Emergency Response Team
<b>ERT-A</b>	Emergency Response Team Advance Element
<b>ERT-N</b>	Emergency Response Team National
<b>ERTU</b>	Evidence Response Team Unit
<b>ESC</b>	Expandable Shelter Container
<b>ESF</b>	Emergency Support Function
<b>ESS</b>	Electronic Security System
<b>EST</b>	Emergency Support Team
<b>ETL</b>	Engineering Technical Letter
<b>EU</b>	explosives unit

# F

<b>FAST</b>	Field Assessment Team
<b>FBI</b>	Federal Bureau of Investigation
<b>FCC</b>	Federal Communications Commission
<b>FCC</b>	Fire Control Center
<b>FCO</b>	Federal Coordinating Officer
<b>FEM</b>	finite element
<b>FEMA</b>	Federal Emergency Management Agency
<b>FEST</b>	Foreign Emergency Support Team
<b>FHBM</b>	Flood Hazard Boundary Map
<b>FIA</b>	Federal Insurance Administration
<b>FIPS</b>	Federal Information Processing Standard
<b>FIRM</b>	Flood Insurance Rate Map
<b>FIS</b>	Flood Insurance Study
<b>FISCAM</b>	Federal Information Systems Control Audit Manual
<b>FMFIA</b>	Federal Manager's Financial Integrity Act
<b>FNS</b>	Food and Nutrition Service
<b>FOIA</b>	Freedom of Information Act
<b>FOUO</b>	For Official Use Only
<b>FPEIS</b>	Final Programmatic Environmental Impact Statement
<b>FRERP</b>	Federal Radiological Emergency Response Plan
<b>FRF</b>	fragment retention film
<b>FRL</b>	Facility Restriction Level

<b>FRMAC</b>	Federal Radiological Monitoring and Assessment Center
<b>FRP</b>	Federal Response Plan
<b>FS</b>	Forest Service
<b>FSTFS</b>	Frame-Supported Tensioned Fabric Structure
<b>FTP</b>	File Transfer Protocol
<b>FTX</b>	Functional Training Exercise



<b>GAO</b>	General Accounting Office
<b>GAR</b>	Governor's Authorized Representative
<b>GC/MS</b>	gas chromatograph/mass spectrometer
<b>GIS</b>	Geographic Information System
<b>GP</b>	General Purpose
<b>GPS</b>	Global Positioning System
<b>GSA</b>	General Services Administration



<b>HazMat</b>	hazardous material
<b>HAZUS</b>	Hazards U.S.
<b>HEPA</b>	high efficiency particulate air
<b>HEU</b>	highly enriched uranium
<b>HF</b>	high frequency
<b>HHS</b>	Department of Health and Human Services

<b>HIRA</b>	Hazard Identification and Risk Assessment
<b>HMRU</b>	Hazardous Materials Response Unit
<b>HQ</b>	Headquarters
<b>HRCQ</b>	Highway Route Controlled Quantity
<b>HRT</b>	Hostage Rescue Team (CIRG)
<b>HTIS</b>	Hazardous Technical Information Services (DoD)
<b>HVAC</b>	heating, ventilation, and air conditioning



<b>IC</b>	Incident Commander
<b>ICDDC</b>	Interstate Civil Defense and Disaster Compact
<b>ICP</b>	Incident Command Post
<b>ICS</b>	Incident Command System
<b>ID</b>	identification
<b>IDS</b>	Intrusion Detection System
<b>IED</b>	Improvised Explosive Device
<b>IEMS</b>	Integrated Emergency Management System
<b>IESNA</b>	Illuminating Engineering Society of North America
<b>IID</b>	Improvised Incendiary Device
<b>IMS</b>	ion mobility spectrometry
<b>IND</b>	Improvised Nuclear Device
<b>IPL</b>	Initial Program Load
<b>IR</b>	infrared
<b>IRZ</b>	Immediate Response Zone

<b>IS</b>	Information System
<b>ISACF</b>	Information Systems Audit and Control Foundation
<b>ISC</b>	Interagency Security Committee
<b>ISO</b>	International Organization for Standardization
<b>ISP</b>	Internet Service Provider
<b>IT</b>	Information Technology

## J

<b>JIC</b>	Joint Information Center
<b>JIIE</b>	Joint Interagency Intelligence Support Element
<b>JIS</b>	Joint Information System
<b>JNACC</b>	Joint Nuclear Accident Coordinating Center
<b>JOC</b>	Joint Operations Center
<b>JSMG</b>	Joint Service Materiel Group
<b>JTF-CS</b>	Joint Task Force for Civil Support
<b>JTTF</b>	Joint Terrorism Task Force
<b>JTWG</b>	Joint Terrorism Working Group

## K

<b>kHz</b>	kilohertz
<b>kPa</b>	kilo Pascal

## L

<b>LAN</b>	Local Area Network
<b>LAW</b>	Light Antitank Weapon
<b>LBNL</b>	Lawrence Berkley National Lab
<b>LCM</b>	Life-cycle Management
<b>LED</b>	light-emitting diode
<b>LEED</b>	Leadership in Energy and Environmental Design
<b>LEPC</b>	Local Emergency Planning Committee
<b>LF</b>	low frequency
<b>LFA</b>	Lead Federal Agency
<b>LLNL</b>	Lawrence Livermore National Laboratory
<b>LOP</b>	level of protection
<b>LOS</b>	line of sight
<b>LPHA</b>	Local Public Health Agency
<b>LPHS</b>	Local Public Health System


## M

<b>MAC</b>	Moves, Adds, Changes
<b>MEDCOM</b>	Medical Command
<b>MEI</b>	Minimum Essential Infrastructure
<b>M/E/P</b>	Mechanical/Electrical/Plumbing
<b>MEP</b>	Mission Essential Process
<b>MERV</b>	minimum efficiency reporting value
<b>MMRS</b>	Metropolitan Medical Response System

<b>MOU/A</b>	Memorandum of Understanding/Agreement
<b>mph</b>	miles per hour
<b>MPOP</b>	Minimum-Points-of-Presence
<b>ms</b>	millisecond
<b>MSCA</b>	Military Support to Civil Authorities
<b>MSDS</b>	Material Safety Data Sheet
<b>MSS</b>	Medium Shelter System
<b>MW</b>	medium wave

## N

<b>NACCHO</b>	National Association for County and City Health Officials
<b>NAP</b>	Nuclear Assessment Program
<b>NAVFAC</b>	Naval Facilities Command
<b>NBC</b>	nuclear, biological, and chemical
<b>NCJ</b>	National Criminal Justice
<b>NCP</b>	National Contingency Plan (also known as National Oil and Hazardous Substances Pollution Contingency Plan)
<b>NDA</b>	National Defense Area
<b>NDMS</b>	National Disaster Medical System
<b>NDPO</b>	National Domestic Preparedness Office
<b>NEST</b>	Nuclear Emergency Search Team
<b>NETC</b>	National Emergency Training Center
<b>NFA</b>	National Fire Academy
<b>NFIP</b>	National Flood Insurance Program

<b>NFPA</b>	National Fire Protection Association
<b>NFPC</b>	National Fire Protection Code
<b>NIJ</b>	National Institute of Justice
<b>NIOSH</b>	National Institute for Occupational Safety and Health
<b>NMRT</b>	National Medical Response Team
<b>NMS</b>	Network Management System
<b>NOAA</b>	National Oceanic and Atmospheric Administration
<b>NRC</b>	National Response Center
<b>NRC</b>	Nuclear Regulatory Commission
<b>NRT</b>	National Response Team
<b>NSC</b>	National Security Council
<b>NTIS</b>	National Technical Information Service
<b>NUREG</b>	Nuclear Regulation
<b>NWS</b>	National Weather Service
	
<b>OCC</b>	Operational Control Center
<b>ODP</b>	Office of Disaster Preparedness
<b>OEP</b>	Office of Emergency Preparedness
<b>OES</b>	Office of Emergency Services
<b>OFCM</b>	Office of the Federal Coordinator for Meteorology
<b>OHS</b>	Office of Homeland Security
<b>OJP</b>	Office of Justice Programs



<b>O&amp;M</b>	operations and maintenance
<b>OMB</b>	Office of Management and Budget
<b>OPA</b>	Oil Pollution Act
<b>OSC</b>	On-scene Coordinator
<b>OSD</b>	Office of Secretary of Defense
<b>OSHA</b>	Occupational Safety and Health Administration
<b>OSLDPS</b>	Office for State and Local Domestic Preparedness Support

## P

<b>Pa</b>	Pascal
<b>PA</b>	public address
<b>PAZ</b>	Protective Action Zone
<b>PBX</b>	Public Branch Exchange
<b>PC</b>	personal computer
<b>PCC</b>	Policy Coordinating Committee
<b>PCCIP</b>	President's Commission on Critical Infrastructure Protection
<b>PCM</b>	Procedures Control Manual
<b>PDA</b>	personal data assistant
<b>PDA</b>	Preliminary Damage Assessment
<b>PDD</b>	Presidential Decision Directive
<b>PHS</b>	Public Health Service
<b>PIN</b>	Personal Identification Number
<b>PIO</b>	Public Information Officer

<b>PL</b>	Public Law
<b>POC</b>	Point of Contact
<b>POD</b>	probability of detection
<b>POI</b>	probability of intrusion
<b>POL</b>	Petroleum, Oils, and Lubricants
<b>POV</b>	privately owned vehicle
<b>PPA</b>	Performance Partnership Agreement
<b>ppm</b>	parts per million
<b>PSE</b>	particle size efficiency
<b>psi</b>	pounds per square inch
<b>PT</b>	Preparedness, Training, and Exercises Directorate (FEMA)
<b>PTE</b>	Potential Threat Element
<b>PTZ</b>	pan-tilt-zoom (camera)
<b>PVB</b>	polyvinyl butyral
<b>PZ</b>	Precautionary Zone

## R

<b>RACES</b>	Radio Amateur Civil Emergency Service
<b>RAP</b>	Radiological Assistance Program
<b>RCRA</b>	Research Conservation and Recovery Act
<b>RDD</b>	Radiological Dispersal Device
<b>RDT&amp;E</b>	Research, Development, Test, and Evaluation
<b>REACT</b>	Radio Emergency Associated Communications Team

<b>REAC/TS</b>	Radiation Emergency Assistance Center/Training Site
<b>REM</b>	Roentgen Man Equivalent
<b>REP</b>	Radiological Emergency Preparedness Program
<b>RF</b>	radio frequency
<b>ROC</b>	Regional Operations Center
<b>ROD</b>	Record of Decision
<b>RPG</b>	Rocket Propelled Grenade
<b>RRIS</b>	Rapid Response Information System (FEMA)
<b>RRP</b>	Regional Response Plan
<b>RRT</b>	Regional Response Team

## S

<b>SAA</b>	State Administrative Agency
<b>SAC</b>	Special Agent in Charge (FBI)
<b>SAFEVU</b>	Safety Viewport Analysis Code
<b>SAME</b>	Specific Area Message Encoder
<b>SARA</b>	Superfund Amendments and Reauthorization Act
<b>SATCOM</b>	satellite communications
<b>SAW</b>	surface acoustic wave
<b>SBCCOM</b>	Soldier and Biological Chemical Command (U.S. Army)
<b>SCADA</b>	Supervisory, Control, and Data Acquisition
<b>SCBA</b>	Self-Contained Breathing Apparatus
<b>SCC</b>	Security Control Center

<b>SCO</b>	State Coordinating Officer
<b>SDOF</b>	single-degree-of-freedom
<b>SEA</b>	Southeast Asia
<b>SEB</b>	State Emergency Board
<b>SEL</b>	Standardized Equipment List
<b>SEMA</b>	State Emergency Management Agency
<b>SERC</b>	State Emergency Response Commission
<b>SFO</b>	Senior FEMA Official
<b>SIOC</b>	Strategic Information and Operations Center (FBI HQ)
<b>SLA</b>	Service Level Agreement
<b>SLG</b>	State and Local Guide
<b>SNM</b>	Special Nuclear Material
<b>SOP</b>	Standard Operating Procedure
<b>SPCA</b>	Society for the Prevention of Cruelty to Animals
<b>SPSA</b>	Super Power Small Arms
<b>SSS</b>	Small Shelter System
<b>STC</b>	Sound Transmission Class
<b>SWAT</b>	Special Weapons and Tactics

## T

<b>TAC</b>	Trunk Access Codes
<b>TDR</b>	transferable development right
<b>TEA</b>	Threat Environment Assessment
<b>TEMPER</b>	Tent, Extendable, Modular, Personnel

<b>TERC</b>	Tribal Emergency Response Commission
<b>TIA</b>	Terrorist Incident Appendix
<b>TIM</b>	toxic industrial material
<b>TM</b>	Technical Manual
<b>TNT</b>	trinitrotoluene
<b>TRIS</b>	Toxic Release Inventory System
<b>TSC</b>	triple-standard concertina
<b>TSO</b>	Time Share Option
<b>TTG</b>	thermally tempered glass

## U

<b>UC</b>	Unified Command
<b>UCS</b>	Unified Command System
<b>UFAS</b>	Uniform Federal Accessibility Standards
<b>UFC</b>	Unified Facilities Criteria
<b>UL</b>	Underwriters Laboratories
<b>ULPA</b>	ultra low penetration air
<b>UPS</b>	uninterrupted power supply
<b>URV</b>	UVGI Rating Values
<b>U.S.</b>	United States
<b>USA</b>	United States Army
<b>USAF</b>	United States Air Force
<b>USC</b>	U.S. Code
<b>USDA</b>	U.S. Department of Agriculture
<b>USFA</b>	U.S. Fire Administration

<b>USGBC</b>	U.S. Green Building Council
<b>USGS</b>	U.S. Geological Survey
<b>US&amp;R</b>	Urban Search and Rescue
<b>UV</b>	ultraviolet
<b>UVGI</b>	ultraviolet germicidal irradiation

## V

<b>VA</b>	Department of Veterans Affairs
<b>VAP</b>	Vulnerability Assessment Plan
<b>VAV</b>	Variable Air Volume
<b>VDN</b>	Vector Directory Number
<b>VHF</b>	very high frequency
<b>VRU</b>	Voice Response Unit

## W

<b>WAN</b>	Wide Area Network
<b>wg</b>	water gauge
<b>WINGARD</b>	Window Glazing Analysis Response and Design
<b>WINLAC</b>	Window Lite Analysis Code
<b>WMD</b>	Weapons of Mass Destruction
<b>WMD-CST</b>	WMD Civil Support Team

This appendix contains some terms that do not actually appear in this manual. They have been included to present a comprehensive list that pertains to this series of publications.

## A

**Access control.** Any combination of barriers, gates, electronic security equipment, and/or guards that can deny entry to unauthorized personnel or vehicles.

**Access control point (ACP).** A station at an entrance to a building or a portion of a building where identification is checked and people and hand-carried items are searched.

**Access controls.** Procedures and controls that limit or detect access to minimum essential infrastructure resource elements (e.g., people, technology, applications, data, and/or facilities), thereby protecting these resources against loss of integrity, confidentiality, accountability, and/or availability.

**Access Control System (ACS).** Also referred to as an Electronic Entry Control Systems; an electronic system that controls entry and egress from a building or area.

**Access Control System elements.** Detection measures used to control vehicle or personnel entry into a protected area. Access Control System elements include locks, Electronic Entry Control Systems, and guards.

**Access group.** A software configuration of an Access Control System that groups together access points or authorized users for easier arrangement and maintenance of the system.

**Access road.** Any roadway such as a maintenance, delivery, service, emergency, or other special limited use road that is necessary for the operation of a building or structure.

**Accountability.** The explicit assignment of responsibilities for oversight of areas of control to executives, managers, staff, owners, providers, and users of minimum essential infrastructure resource elements.

**Acoustic eavesdropping.** The use of listening devices to monitor voice communications or other audibly transmitted information with the objective to compromise information.

**Active vehicle barrier.** An impediment placed at an access control point that may be manually or automatically deployed in response to detection of a threat.

**Aerosol.** Fine liquid or solid particles suspended in a gas (e.g., fog or smoke).

**Aggressor.** Any person seeking to compromise a function or structure.

**Airborne contamination.** Chemical or biological agents introduced into and fouling the source of supply of breathing or conditioning air.

**Airlock.** A building entry configuration with which airflow from the outside can be prevented from entering a toxic-free area. An airlock uses two doors, only one of which can be opened at a time, and a blower system to maintain positive air pressures and purge contaminated air from the airlock before the second door is opened.

**Alarm assessment.** Verification and evaluation of an alarm alert through the use of closed circuit television or human observation. Systems used for alarm assessment are designed to respond rapidly, automatically, and predictably to the receipt of alarms at the security center.

**Alarm printers.** Alarm printers provide a hard-copy of all alarm events and system activity, as well as limited backup in case the visual display fails.

**Alarm priority.** A hierarchy of alarms by order of importance. This is often used in larger systems to give priority to alarms with greater importance.



**Annunciation.** A visual, audible, or other indication by a security system of a condition.

**Antiterrorism (AT).** Defensive measures used to reduce the vulnerability of individuals, forces, and property to terrorist acts.

**Area Commander.** A military commander with authority in a specific geographical area or military installation.

**Area lighting.** Lighting that illuminates a large exterior area.

**Areas of potential compromise.** Categories where losses can occur that will impact either a department's or an agency's minimum essential infrastructure and its ability to conduct core functions and activities.

**Assessment.** The evaluation and interpretation of measurements and other information to provide a basis for decision-making.

**Assessment System elements.** Detection measures used to assist guards in visual verification of Intrusion Detection System Alarms and Access Control System functions and to assist in visual detection by guards. Assessment System elements include closed circuit television and protective lighting.

**Asset.** A resource of value requiring protection. An asset can be tangible (e.g., people, buildings, facilities, equipment, activities, operations, and information) or intangible (e.g., processes or a company's information and reputation).

**Asset protection.** Security program designed to protect personnel, facilities, and equipment, in all locations and situations, accomplished through planned and integrated application of combating terrorism, physical security, operations security, and personal protective services, and supported by intelligence, counterintelligence, and other security programs.

**Asset value.** The degree of debilitating impact that would be caused by the incapacity or destruction of an asset.

**Attack.** A hostile action resulting in the destruction, injury, or death to the civilian population, or damage or destruction to public and private property.

**Audible alarm device.** An alarm device that produces an audible announcement (e.g., bell, horn, siren, etc.) of an alarm condition.

## B

**Balanced magnetic switch.** A door position switch utilizing a reed switch held in a balanced or center position by interacting magnetic fields when not in alarm condition.

**Ballistics attack.** An attack in which small arms (e.g., pistols, submachine guns, shotguns, and rifles) are fired from a distance and rely on the flight of the projectile to damage the target.

**Barbed tape or concertina.** A coiled tape or coil of wires with wire barbs or blades deployed as an obstacle to human trespass or entry into an area.

**Barbed wire.** A double strand of wire with four-point barbs equally spaced along the wire deployed as an obstacle to human trespass or entry into an area.

**Barcode.** A black bar printed on white paper or tape that can be easily read with an optical scanner.

**Biological agents.** Living organisms or the materials derived from them that cause disease in or harm to humans, animals, or plants or cause deterioration of material. Biological agents may be used as liquid droplets, aerosols, or dry powders.

**Biometric reader.** A device that gathers and analyzes biometric features.

**Biometrics.** The use of physical characteristics of the human body as a unique identification method.

**Blast curtains.** Heavy curtains made of blast-resistant materials that could protect the occupants of a room from flying debris.

**Blast-resistant glazing.** Window opening glazing that is resistant to blast effects because of the interrelated function of the frame and

glazing material properties frequently dependent upon tempered glass, polycarbonate, or laminated glazing.

**Blast vulnerability envelope.** The geographical area in which an explosive device will cause damage to assets.

**Bollard.** A vehicle barrier consisting of a cylinder, usually made of steel and sometimes filled with concrete, placed on end in the ground and spaced about 3 feet apart to prevent vehicles from passing, but allowing entrance of pedestrians and bicycles.

**Boundary penetration sensor.** An interior intrusion detection sensor that detects attempts by individuals to penetrate or enter a building.

**Building hardening.** Enhanced construction that reduces vulnerability to external blast and ballistic attacks.

**Building separation.** The distance between closest points on the exterior walls of adjacent buildings or structures.

**Business Continuity Program (BCP).** An ongoing process supported by senior management and funded to ensure that the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies and recovery plans, and ensure continuity services through personnel training, plan testing, and maintenance.



**Cable barrier.** Cable or wire rope anchored to and suspended off the ground or attached to chain-link fence to act as a barrier to moving vehicles.

**Capacitance sensor.** A device that detects an intruder approaching or touching a metal object by sensing a change in capacitance between the object and the ground.

**Card reader.** A device that gathers or reads information when a card is presented as an identification method.

**Chemical agent.** A chemical substance that is intended to kill, seriously injure, or incapacitate people through physiological effects. Generally separated by severity of effect (e.g., lethal, blister, and incapacitating).

**Chimney effect.** Air movement in a building between floors caused by differential air temperature (differences in density), between the air inside and outside the building. It occurs in vertical shafts, such as elevators, stairwells, and conduit/wiring/piping chases. Hotter air inside the building will rise and be replaced by infiltration with colder outside air through the lower portions of the building. Conversely, reversing the temperature will reverse the flow (down the chimney). Also known as stack effect.

**Clear zone.** An area that is clear of visual obstructions and landscape materials that could conceal a threat or perpetrator.

**Closed circuit television (CCTV).** An electronic system of cameras, control equipment, recorders, and related apparatus used for surveillance or alarm assessment.

**CCTV pan-tilt-zoom camera (PTZ).** A CCTV camera that can move side to side, up and down, and zoom in or out.

**CCTV pan-tilt-zoom control.** The method of controlling the PTZ functions of a camera.

**CCTV pan-tilt-zoom controller.** The operator interface for performing PTZ control.

**CCTV switcher.** A piece of equipment capable of presenting multiple video images to various monitors, recorders, etc.

**Collateral damage.** Injury or damage to assets that are not the primary target of an attack.

**Combating terrorism.** The full range of federal programs and activities applied against terrorism, domestically and abroad, regardless of the source or motive.

**Community.** A political entity that has the authority to adopt and enforce laws and ordinances for the area under its jurisdiction. In most cases, the community is an incorporated town, city, township, village, or unincorporated area of a county; however, each state defines its own political subdivisions and forms of government.

**Components and cladding.** Elements of the building envelope that do not qualify as part of the main wind-force resisting system.

**Confidentiality.** The protection of sensitive information against unauthorized disclosure and sensitive facilities from physical, technical, or electronic penetration or exploitation.

**Consequence Management.** Measures to protect public health and safety, restore essential government services, and provide emergency relief to governments, businesses, and individuals affected by the consequences of terrorism. State and local governments exercise the primary authority to respond to the consequences of terrorism.

**Contamination.** The undesirable deposition of a chemical, biological, or radiological material on the surface of structures, areas, objects, or people.

**Continuity of services and operations.** Controls to ensure that, when unexpected events occur, departmental/agency minimum essential infrastructure services and operations, including computer operations, continue without interruption or are promptly resumed, and that critical and sensitive data are protected through adequate contingency and business recovery plans and exercises.

**Control center.** A centrally located room or facility staffed by personnel charged with the oversight of specific situations and/or equipment.

**Controlled area.** An area into which access is controlled or limited. It is that portion of a restricted area usually near or surrounding a limited or exclusion area. Correlates with exclusion zone.

**Controlled lighting.** Illumination of specific areas or sections.

**Controlled perimeter.** A physical boundary at which vehicle and personnel access is controlled at the perimeter of a site. Access control at a controlled perimeter should demonstrate the capability to search individuals and vehicles.

**Conventional construction.** Building construction that is not specifically designed to resist weapons, explosives, or chemical, biological, and radiological effects. Conventional construction is designed only to resist common loadings and environmental effects such as wind, seismic, and snow loads.

**Coordinate.** To advance systematically an exchange of information among principals who have or may have a need to know certain information in order to carry out their roles in a response.

**Counterintelligence.** Information gathered and activities conducted to protect against: espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons; or international terrorist activities, excluding personnel, physical, document, and communications security programs.

**Counterterrorism (CT).** Offensive measures taken to prevent, deter, and respond to terrorism.

**Covert entry.** Attempts to enter a facility by using false credentials or stealth.

**Crash bar.** A mechanical egress device located on the interior side of a door that unlocks the door when pressure is applied in the direction of egress.

**Crime Prevention Through Environmental Design (CPTED).** A crime prevention strategy based on evidence that the design and form of the built environment can influence human behavior. CPTED usually involves the use of three principles: natural surveillance (by placing physical features, activities, and people to maximize visibility); natural access control (through the judicious placement of entrances, exits, fencing, landscaping, and lighting); and territorial reinforcement (using buildings, fences, pavement, signs, and landscaping to express ownership).

**Crisis Management (CM).** The measures taken to identify, acquire, and plan the use of resources needed to anticipate, prevent, and/or resolve a threat or act of terrorism.

**Critical assets.** Those assets essential to the minimum operations of the organization, and to ensure the health and safety of the general public.

**Critical infrastructure.** Primary infrastructure systems (e.g., utilities, telecommunications, transportation, etc.) whose incapacity would have a debilitating impact on the organization's ability to function.

## D

**Damage assessment.** The process used to appraise or determine the number of injuries and deaths, damage to public and private property, and the status of key facilities and services (e.g., hospitals and other health care facilities, fire and police stations, communications networks, water and sanitation systems, utilities, and transportation networks) resulting from a manmade or natural disaster.

**Data gathering panel.** A local processing unit that retrieves, processes, stores, and/or acts on information in the field.

**Data transmission equipment.** A path for transmitting data between two or more components (e.g., a sensor and alarm reporting system, a card reader and controller, a CCTV camera and monitor, or a transmitter and receiver).

**Decontamination.** The reduction or removal of a chemical, biological, or radiological material from the surface of a structure, area, object, or person.

**Defense layer.** Building design or exterior perimeter barriers intended to delay attempted forced entry.

**Defensive measures.** Protective measures that delay or prevent attack on an asset or that shield the asset from weapons, explosives, and CBR effects. Defensive measures include site work and building design.

**Delay rating.** A measure of the effectiveness of penetration protection of a defense layer.

**Design Basis Threat (DBT).** The threat (e.g., tactics and associated weapons, tools, or explosives) against which assets within a building must be protected and upon which the security engineering design of the building is based.

**Design constraint.** Anything that restricts the design options for a protective system or that creates additional problems for which the design must compensate.

**Design opportunity.** Anything that enhances protection, reduces requirements for protective measures, or solves a design problem.

**Design team.** A group of individuals from various engineering and architectural disciplines responsible for the protective system design.

**Detection layer.** A ring of intrusion detection sensors located on or adjacent to a defensive layer or between two defensive layers.

**Detection measures.** Protective measures that detect intruders, weapons, or explosives; assist in assessing the validity of detection; control access to protected areas; and communicate the appropriate information to the response force. Detection measures include Detection Systems, Assessment Systems, and Access Control System elements.

**Detection System elements.** Detection measures that detect the presence of intruders, weapons, or explosives. Detection System elements include Intrusion Detection Systems, weapons and explosives detectors, and guards.

**Disaster.** An occurrence of a natural catastrophe, technological accident, or human-caused event that has resulted in severe property damage, deaths, and/or multiple injuries.



**Disaster Field Office (DFO).** The office established in or near the designated area of a Presidentially declared major disaster to support federal and state response and recovery operations.

**Disaster Recovery Center (DRC).** Places established in the area of a Presidentially declared major disaster, as soon as practicable, to provide victims the opportunity to apply in person for assistance and/or obtain information relating to that assistance.

**Domestic terrorism.** The unlawful use, or threatened use, of force or violence by a group or individual based and operating entirely within the United States or Puerto Rico without foreign direction committed against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof in furtherance of political or social objectives.

**Door position switch.** A switch that changes state based on whether or not a door is closed. Typically, a switch mounted in a frame that is actuated by a magnet in a door.

**Door strike, electronic.** An electromechanical lock that releases a door plunger to unlock the door. Typically, an electronic door strike is mounted in place of or near a normal door strike plate.

**Dose rate (radiation).** A general term indicating the quantity (total or accumulated) of ionizing radiation or energy absorbed by a person or animal, per unit of time.

**Dosimeter.** An instrument for measuring and registering total accumulated exposure to ionizing radiation.

**Dual technology sensor.** A sensor that combines two different technologies in one unit.

**Duress alarm devices.** Also known as panic buttons, these devices are designated specifically to initiate a panic alarm.

# E

**Effective stand-off distance.** A stand-off distance at which the required level of protection can be shown to be achieved through analysis or can be achieved through building hardening or other mitigating construction or retrofit.

**Electromagnetic pulse (EMP).** A sharp pulse of energy radiated instantaneously by a nuclear detonation that may affect or damage electronic components and equipment. EMP can also be generated in lesser intensity by non-nuclear means in specific frequency ranges to perform the same disruptive function.

**Electronic emanations.** Electromagnetic emissions from computers, communications, electronics, wiring, and related equipment.

**Electronic-emanations eavesdropping.** Use of electronic-emanation surveillance equipment from outside a facility or its restricted area to monitor electronic emanations from computers, communications, and related equipment.

**Electronic Entry Control Systems (EECS).** Electronic devices that automatically verify authorization for a person to enter or exit a controlled area.

**Electronic Security System (ESS).** An integrated system that encompasses interior and exterior sensors, closed circuit television systems for assessment of alarm conditions, Electronic Entry Control Systems, data transmission media, and alarm reporting systems for monitoring, control, and display of various alarm and system information.

**Emergency.** Any natural or human-caused situation that results in or may result in substantial injury or harm to the population or substantial damage to or loss of property.

**Emergency Alert System (EAS).** A communications system of broadcast stations and interconnecting facilities authorized by the Federal Communications Commission (FCC). The system provides the President and other national, state, and local

officials the means to broadcast emergency information to the public before, during, and after disasters.

**Emergency Environmental Health Services.** Services required to correct or improve damaging environmental health effects on humans, including inspection for food contamination, inspection for water contamination, and vector control; providing for sewage and solid waste inspection and disposal; cleanup and disposal of hazardous materials; and sanitation inspection for emergency shelter facilities.

**Emergency Medical Services (EMS).** Services including personnel, facilities, and equipment required to ensure proper medical care for the sick and injured from the time of injury to the time of final disposition, including medical disposition within a hospital, temporary medical facility, or special care facility; release from the site; or declared dead. Further, Emergency Medical Services specifically include those services immediately required to ensure proper medical care and specialized treatment for patients in a hospital and coordination of related hospital services.

**Emergency Mortuary Services.** Services required to assure adequate death investigation, identification, and disposition of bodies; removal, temporary storage, and transportation of bodies to temporary morgue facilities; notification of next of kin; and coordination of mortuary services and burial of unclaimed bodies.

**Emergency Operations Center (EOC).** The protected site from which state and local civil government officials coordinate, monitor, and direct emergency response activities during an emergency.

**Emergency Operations Plan (EOP).** A document that describes how people and property will be protected in disaster and disaster threat situations; details who is responsible for carrying out specific actions; identifies the personnel, equipment, facilities, supplies, and other resources available for use in the disaster; and outlines how all actions will be coordinated.

**Emergency Planning Zones (EPZ).** Areas around a facility for which planning is needed to ensure prompt and effective actions are taken to protect the health and safety of the public

if an accident or disaster occurs. In the Radiological Emergency Preparedness Program, the two EPZs are:

**Plume Exposure Pathway (10-mile EPZ).** A circular geographic zone (with a 10-mile radius centered at the nuclear power plant) for which plans are developed to protect the public against exposure to radiation emanating from a radioactive plume caused as a result of an accident at the nuclear power plant.

**Ingestion Pathway (50-mile EPZ).** A circular geographic zone (with a 50-mile radius centered at the nuclear power plant) for which plans are developed to protect the public from the ingestion of water or food contaminated as a result of a nuclear power plant accident.

In the Chemical Stockpile Emergency Preparedness Program (CSEPP), the EPZ is divided into three concentric circular zones:

**Immediate Response Zone (IRZ).** A circular zone ranging from 10 to 15 kilometers (6 to 9 miles) from the potential chemical event source, depending on the stockpile location on-post. Emergency response plans developed for the IRZ must provide for the most rapid and effective protective actions possible, because the IRZ will have the highest concentration of agent and the least amount of warning time.

**Protective Action Zone (PAZ).** An area that extends beyond the IRZ to approximately 16 to 50 kilometers (10 to 30 miles) from the stockpile location. The PAZ is that area where public protective actions may still be necessary in case of an accidental release of chemical agent, but where the available warning and response time is such that most people could evacuate. However, other responses (e.g., sheltering) may be appropriate for institutions and special populations that could not evacuate within the available time.

**Precautionary Zone (PZ).** The outermost portion of the EPZ for CSEPP, extending from the PAZ outer boundary to a distance where the risk of adverse impacts to humans is negligible. Because of the increased warning and response time available for implementation of response actions in the PZ, detailed local emergency planning is not required, although Consequence Management planning may be appropriate.

**Emergency Public Information (EPI).** Information that is disseminated primarily in anticipation of an emergency or at the actual time of an emergency and, in addition to providing information, frequently directs actions, instructs, and transmits direct orders.

**Emergency Response Team (ERT).** An interagency team, consisting of the lead representative from each federal department or agency assigned primary responsibility for an ESF and key members of the FCO's staff, formed to assist the FCO in carrying out his/her coordination responsibilities.

**Emergency Response Team Advance Element (ERT-A).** For federal disaster response and recovery activities under the Stafford Act, the portion of the ERT that is first deployed to the field to respond to a disaster incident. The ERT-A is the nucleus of the full ERT.

**Emergency Response Team National (ERT-N).** An ERT that has been established and rostered for deployment to catastrophic disasters where the resources of the FEMA Region have been, or are expected to be, overwhelmed. Three ERT-Ns have been established.

**Emergency Support Function (ESF).** In the Federal Response Plan (FRP), a functional area of response activity established to facilitate the delivery of federal assistance required during the immediate response phase of a disaster to save lives, protect property and public health, and to maintain public safety. ESFs represent those types of federal assistance that the state will most likely need because of the impact of a catastrophic or significant disaster on its own resources and response capabilities,

or because of the specialized or unique nature of the assistance required. ESF missions are designed to supplement state and local response efforts.

**Emergency Support Team (EST).** An interagency group operating from FEMA Headquarters. The EST oversees the national-level response support effort under the FRP and coordinates activities with the ESF primary and support agencies in supporting federal requirements in the field.

**Entity-wide security.** Planning and management that provides a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the entity's physical and cyber security controls.

**Entry control point.** A continuously or intermittently manned station at which entry to sensitive or restricted areas is controlled.

**Entry control stations.** Entry control stations should be provided at main perimeter entrances where security personnel are present. Entry control stations should be located as close as practical to the perimeter entrance to permit personnel inside the station to maintain constant surveillance over the entrance and its approaches.

**Equipment closet.** A room where field control equipment such as data gathering panels and power supplies are typically located.

**Evacuation.** Organized, phased, and supervised dispersal of people from dangerous or potentially dangerous areas.

**Evacuation, mandatory or directed.** This is a warning to persons within the designated area that an imminent threat to life and property exists and individuals **MUST** evacuate in accordance with the instructions of local officials.

**Evacuation, spontaneous.** Residents or citizens in the threatened areas observe an emergency event or receive unofficial word of an actual or perceived threat and, without receiving instructions to do so, elect to evacuate the area. Their movement, means, and direction of travel are unorganized and unsupervised.

**Evacuation, voluntary.** This is a warning to persons within a designated area that a threat to life and property exists or is likely to exist in the immediate future. Individuals issued this type of warning or order are NOT required to evacuate; however, it would be to their advantage to do so.

**Evacuees.** All persons removed or moving from areas threatened or struck by a disaster.

**Exclusion area.** A restricted area containing a security interest. Uncontrolled movement permits direct access to the item. See controlled area and limited area.

**Exclusion zone.** An area around an asset that has controlled entry with highly restrictive access. See controlled area.

**Explosives disposal container.** A small container into which small quantities of explosives may be placed to contain their blast pressures and fragments if the explosive detonates.

## F

**Facial recognition.** A biometric technology that is based on features of the human face.

**Federal Coordinating Officer (FCO).** The person appointed by the FEMA Director to coordinate federal assistance in a Presidentially declared emergency or major disaster.

**Federal On-scene Commander.** The FBI official designated upon JOC activation to ensure appropriate coordination of the overall United States government response with federal, state, and local authorities, until such time as the Attorney General transfers the LFA role to FEMA.

**Federal Response Plan (FRP).** The FRP establishes a process and structure for the systematic, coordinated, and effective delivery of federal assistance to address the consequences of any major disaster or emergency.

**Fence protection.** An intrusion detection technology that detects a person crossing a fence by various methods such as climbing, crawling, cutting, etc.

**Fence sensor.** An exterior intrusion detection sensor that detects aggressors as they attempt to climb over, cut through, or otherwise disturb a fence.

**Fiber optics.** A method of data transfer by passing bursts of light through a strand of glass or clear plastic.

**Field Assessment Team (FAsT).** A small team of pre-identified technical experts that conduct an assessment of response needs (not a PDA) immediately following a disaster.

**Field of view.** The visible area in a video picture.

**First responder.** Local police, fire, and emergency medical personnel who first arrive on the scene of an incident and take action to save lives, protect property, and meet basic human needs.

**Flash flood.** Follows a situation in which rainfall is so intense and severe and runoff so rapid that it precludes recording and relating it to stream stages and other information in time to forecast a flood condition.

**Flood.** A general and temporary condition of partial or complete inundation of normally dry land areas from overflow of inland or tidal waters, unusual or rapid accumulation or runoff of surface waters, or mudslides/mudflows caused by accumulation of water.

**Forced entry.** Entry to a denied area achieved through force to create an opening in fence, walls, doors, etc., or to overpower guards.

**Fragment retention film (FRF).** A thin, optically clear film applied to glass to minimize the spread of glass fragments when the glass is shattered.

**Frame rate.** In digital video, a measurement of the rate of change in a series of pictures, often measured in frames per second (fps).

**Frangible construction.** Building components that are designed to fail to vent blast pressures from an enclosure in a controlled manner and direction.





**Glare security lighting.** Illumination projected from a secure perimeter into the surrounding area, making it possible to see potential intruders at a considerable distance while making it difficult to observe activities within the secure perimeter.

**Glass-break detector.** An intrusion detection sensor that is designed to detect breaking glass either through vibration or acoustics.

**Glazing.** A material installed in a sash, ventilator, or panes (e.g., glass, plastic, etc., including material such as thin granite installed in a curtain wall).

**Governor's Authorized Representative (GAR).** The person empowered by the Governor to execute, on behalf of the State, all necessary documents for disaster assistance.

**Grid wire sensor.** An intrusion detection sensor that uses a grid of wires to cover a wall or fence. An alarm is sounded if the wires are cut.



**Hand geometry.** A biometric technology that is based on characteristics of the human hand.

**Hazard.** A source of potential danger or adverse condition.

**Hazard mitigation.** Any action taken to reduce or eliminate the long-term risk to human life and property from hazards. The term is sometimes used in a stricter sense to mean cost-effective measures to reduce the potential for damage to a facility or facilities from a disaster event.

**Hazardous material (HazMat).** Any substance or material that, when involved in an accident and released in sufficient quantities, poses a risk to people's health, safety, and/or property. These substances and materials include explosives, radioactive materials,

flammable liquids or solids, combustible liquids or solids, poisons, oxidizers, toxins, and corrosive materials.

**High-hazard areas.** Geographic locations that, for planning purposes, have been determined through historical experience and vulnerability analysis to be likely to experience the effects of a specific hazard (e.g., hurricane, earthquake, hazardous materials accident, etc.), resulting in vast property damage and loss of life.

**High-risk target.** Any material resource or facility that, because of mission sensitivity, ease of access, isolation, and symbolic value, may be an especially attractive or accessible terrorist target.

**Human-caused hazard.** Human-caused hazards are technological hazards and terrorism. They are distinct from natural hazards primarily in that they originate from human activity. Within the military services, the term threat is typically used for human-caused hazard. See definitions of technological hazards and terrorism for further information.

**Hurricane.** A tropical cyclone, formed in the atmosphere over warm ocean areas, in which wind speeds reach 74 miles per hour or more and blow in a large spiral around a relatively calm center or “eye.” Circulation is counter-clockwise in the Northern Hemisphere and clockwise in the Southern Hemisphere.



**Impact analysis.** A management level analysis that identifies the impacts of losing the entity’s resources. The analysis measures the effect of resource loss and escalating losses over time in order to provide the entity with reliable data upon which to base decisions on hazard mitigation and continuity planning.

**Incident Command System (ICS).** A standardized organizational structure used to command, control, and coordinate the use of resources and personnel that have responded to the scene of an emergency. The concepts and principles for ICS include common

terminology, modular organization, integrated communication, unified command structure, consolidated action plan, manageable span of control, designated incident facilities, and comprehensive resource management.

**Insider compromise.** A person authorized access to a facility (an insider) compromises assets by taking advantage of that accessibility.

**Intercom door/gate station.** Part of an intercom system where communication is typically initiated, usually located at a door or gate.

**Intercom master station.** Part of an intercom system that monitors one or more intercom door/gate stations; typically, where initial communication is received.

**Intercom switcher.** Part of an intercom system that controls the flow of communications between various stations.

**Intercom System.** An electronic system that allows simplex, half-duplex, or full-duplex audio communications.

**International terrorism.** Violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or any state, or that would be a criminal violation if committed within the jurisdiction of the United States or any state. These acts appear to be intended to intimidate or coerce a civilian population, influence the policy of a government by intimidation or coercion, or affect the conduct of a government by assassination or kidnapping. International terrorist acts occur outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

**Intrusion Detection Sensor.** A device that initiates alarm signals by sensing the stimulus, change, or condition for which it was designed.

**Intrusion Detection System (IDS).** The combination of components, including sensors, control units, transmission lines, and monitor units, integrated to operate in a specified manner.

**Isolated fenced perimeters.** Fenced perimeters with 100 feet or more of space outside the fence that is clear of obstruction, making approach obvious.



**Jersey barrier.** A protective concrete barrier initially and still used as a highway divider that now also functions as an expedient method for traffic speed control at entrance gates and to keep vehicles away from buildings.

**Joint Information Center (JIC).** A central point of contact for all news media near the scene of a large-scale disaster. News media representatives are kept informed of activities and events by Public Information Officers who represent all participating federal, state, and local agencies that are collocated at the JIC.

**Joint Information System (JIS).** Under the FRP, connection of public affairs personnel, decision-makers, and news centers by electronic mail, fax, and telephone when a single federal-state-local JIC is not a viable option.

**Joint Interagency Intelligence Support Element (JIISE).** An inter-agency intelligence component designed to fuse intelligence information from the various agencies participating in a response to a WMD threat or incident within an FBI JOC. The JIISE is an expanded version of the investigative/intelligence component that is part of the standardized FBI command post structure. The JIISE manages five functions, including: security, collections management, current intelligence, exploitation, and dissemination.

**Joint Operations Center (JOC).** Established by the LFA under the operational control of the federal OSC, as the focal point for management and direction of on-site activities, coordination/establishment of state requirements/priorities, and coordination of the overall federal response.

**Jurisdiction.** Typically counties and cities within a state, but states may elect to define differently in order to facilitate their assessment process.



**Laminated glass.** A flat lite of uniform thickness consisting of two monolithic glass plies bonded together with an interlayer material as defined in Specification C1172. Many different interlayer materials are used in laminated glass.

**Landscaping.** The use of plantings (shrubs and trees), with or without landforms and/or large boulders, to act as a perimeter barrier against defined threats.

**Laser card.** A card technology that uses a laser reflected off of a card for uniquely identifying the card.

**Layers of protection.** A traditional approach in security engineering using concentric circles extending out from an area to be protected as demarcation points for different security strategies.

**Lead Agency.** The federal department or agency assigned lead responsibility under U.S. law to manage and coordinate the federal response in a specific functional area.

**Lead Federal Agency (LFA).** The agency designated by the President to lead and coordinate the overall federal response is referred to as the LFA and is determined by the type of emergency. In general, an LFA establishes operational structures and procedures to assemble and work with agencies providing direct support to the LFA in order to provide an initial assessment of the situation, develop an action plan, monitor and update operational priorities, and ensure each agency exercises its concurrent and distinct authorities under U.S. law and supports the LFA in carrying out the President's relevant policy. Specific responsibilities of an LFA vary, according to the agency's unique statutory authorities.

**Level of protection (LOP).** The degree to which an asset is protected against injury or damage from an attack.

**Liaison.** An agency official sent to another agency to facilitate interagency communications and coordination.

**Limited area.** A restricted area within close proximity of a security interest. Uncontrolled movement may permit access to the item. Escorts and other internal restrictions may prevent access to the item. See controlled area and exclusion area.

**Line of sight (LOS).** Direct observation between two points with the naked eye or hand-held optics.

**Line-of-sight sensor.** A pair of devices used as an intrusion detection sensor that monitor any movement through the field between the sensors.

**Line supervision.** A data integrity strategy that monitors the communications link for connectivity and tampering. In Intrusion Detection System sensors, line supervision is often referred to as two-state, three-state, or four-state in respect to the number of conditions monitored. The frequency of sampling the link also plays a big part in the supervision of the line.

**Local government.** Any county, city, village, town, district, or political subdivision of any state, and Indian tribe or authorized tribal organization, or Alaska Native village or organization, including any rural community or unincorporated town or village or any other public entity.

## M

**Magnetic lock.** An electromagnetic lock that unlocks a door when power is removed.

**Magnetic stripe.** A card technology that uses a magnetic stripe on the card to encode data used for unique identification of the card.

**Mail-bomb delivery.** Bombs or incendiary devices delivered to the target in letters or packages.

**Man-trap.** An access control strategy that uses a pair of interlocking doors to prevent tailgating. Only one door can be unlocked at a time.

**Mass care.** The actions that are taken to protect evacuees and other disaster victims from the effects of the disaster. Activities include providing temporary shelter, food, medical care, clothing, and other essential life support needs to those people who have been displaced from their homes because of a disaster or threatened disaster.

**Mass notification.** Capability to provide real-time information to all building occupants or personnel in the immediate vicinity of a building during emergency situations.

**Microwave motion sensor.** An intrusion detection sensor that uses microwave energy to sense movement within the sensor's field of view. These sensors work similar to radar by using the Doppler effect to measure a shift in frequency.

**Military installations.** Army, Navy, Air Force, and Marine Corps bases, posts, stations, and annexes (both contractor and government operated), hospitals, terminals, and other special mission facilities, as well as those used primarily for military purposes.

**Minimum essential infrastructure resource elements.** The broad categories of resources, all or portions of which constitute the minimal essential infrastructure necessary for a department, agency, or organization to conduct its core mission(s).

**Minimum measures.** Protective measures that can be applied to all buildings regardless of the identified threat. These measures offer defense or detection opportunities for minimal cost, facilitate future upgrades, and may deter acts of aggression.

**Mitigation.** Those actions taken to reduce the exposure to and impact of an attack or disaster.

**Motion detector.** An intrusion detection sensor that changes state based on movement in the sensor's field of view.

**Moving vehicle bomb.** An explosive-laden car or truck driven into or near a building and detonated.

**Mutual Aid Agreement.** A pre-arranged agreement developed between two or more entities to render assistance to the parties of the agreement.

## N

**Natural hazard.** Naturally-occurring events such as floods, earthquakes, tornadoes, tsunamis, coastal storms, landslides, and wildfires that strike populated areas. A natural event is a hazard when it has the potential to harm people or property (FEMA 386-2, *Understanding Your Risks*). The risks of natural hazards may be increased or decreased as a result of human activity; however, they are not inherently human-induced.

**Natural protective barriers.** Natural protective barriers are mountains and deserts, cliffs and ditches, water obstacles, or other terrain features that are difficult to traverse.

**Non-exclusive zone.** An area around an asset that has controlled entry, but shared or less restrictive access than an exclusive zone.

**Non-persistent agent.** An agent that, upon release, loses its ability to cause casualties after 10 to 15 minutes. It has a high evaporation rate, is lighter than air, and will disperse rapidly. It is considered to be a short-term hazard; however, in small, unventilated areas, the agent will be more persistent.

**Nuclear, biological, or chemical weapons.** Also called Weapons of Mass Destruction (WMD). Weapons that are characterized by their capability to produce mass casualties.

**Nuclear detonation.** An explosion resulting from fission and/or fusion reactions in nuclear material, such as that from a nuclear weapon.





**On-Scene Coordinator (OSC).** The federal official pre-designated by the EPA and U.S. Coast Guard to coordinate and direct response and removals under the National Oil and Hazardous Substances Pollution Contingency Plan.

**Open systems architecture.** A term borrowed from the IT industry to claim that systems are capable of interfacing with other systems from any vendor, which also uses open system architecture. The opposite would be a proprietary system.

**Operator interface.** The part of a security management system that provides that user interface to humans.

**Organizational areas of control.** Controls consist of the policies, procedures, practices, and organization structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected.



**Passive infrared motion sensor.** A device that detects a change in the thermal energy pattern caused by a moving intruder and initiates an alarm when the change in energy satisfies the detector's alarm-criteria.

**Passive vehicle barrier.** A vehicle barrier that is permanently deployed and does not require response to be effective.

**Patch panel.** A concentrated termination point that separates backbone cabling from devices cabling for easy maintenance and troubleshooting.

**Perimeter barrier.** A fence, wall, vehicle barrier, landform, or line of vegetation applied along an exterior perimeter used to obscure vision, hinder personnel access, or hinder or prevent vehicle access.

**Persistent agent.** An agent that, upon release, retains its casualty-producing effects for an extended period of time, usually anywhere from 30 minutes to several days. A persistent agent usually has a low evaporation rate and its vapor is heavier than air; therefore, its vapor cloud tends to hug the ground. It is considered to be a long-term hazard. Although inhalation hazards are still a concern, extreme caution should be taken to avoid skin contact as well.

**Physical security.** The part of security concerned with measures/concepts designed to safeguard personnel; to prevent unauthorized access to equipment, installations, materiel, and documents; and to safeguard them against espionage, sabotage, damage, and theft.

**Planter barrier.** A passive vehicle barrier, usually constructed of concrete and filled with dirt (and flowers for aesthetics). Planters, along with bollards, are the usual street furniture used to keep vehicles away from existing buildings. Overall size and the depth of installation below grade determine the vehicle stopping capability of the individual planter.

**Plume.** Airborne material spreading from a particular source; the dispersal of particles, gases, vapors, and aerosols into the atmosphere.

**Polycarbonate glazing.** A plastic glazing material with enhanced resistance to ballistics or blast effects.

**Predetonation screen.** A fence that causes an anti-tank round to detonate or prevents it from arming before it reaches its target.

**Preliminary Damage Assessment (PDA).** A mechanism used to determine the impact and magnitude of damage and the resulting unmet needs of individuals, businesses, the public sector, and the community as a whole. Information collected is used by the state as a basis for the Governor's request for a Presidential declaration, and by FEMA to document the recommendation made to the President in response to the Governor's request. PDAs are made by at least one state and one federal representative. A local government representative familiar with the extent and location of damage in the community

often participates; other state and federal agencies and voluntary relief organizations also may be asked to participate, as needed.

**Preparedness.** Establishing the plans, training, exercises, and resources necessary to enhance mitigation of and achieve readiness for response to, and recovery from all hazards, disasters, and emergencies, including WMD incidents.

**Pressure mat.** A mat that generates an alarm when pressure is applied to any part of the mat's surface, such as when someone steps on the mat. Pressure mats can be used to detect an intruder approaching a protected object, or they can be placed by doors and windows to detect entry.

**Primary asset.** An asset that is the ultimate target for compromise by an aggressor.

**Primary gathering building.** Inhabited buildings routinely occupied by 50 or more personnel. This designation applies to the entire portion of a building that meets the population density requirements for an inhabited building.

**Probability of detection (POD).** A measure of an intrusion detection sensor's performance in detecting an intruder within its detection zone.

**Probability of intercept.** The probability that an act of aggression will be detected and that a response force will intercept the aggressor before the asset can be compromised.

**Progressive collapse.** A chain reaction failure of building members to an extent disproportionate to the original localized damage. Such damage may result in upper floors of a building collapsing onto lower floors.

**Protective barriers.** Define the physical limits of a site, activity, or area by restricting, channeling, or impeding access and forming a continuous obstacle around the object.

**Protective measures.** Elements of a protective system that protect an asset against a threat. Protective measures are divided into defensive and detection measures.

**Protective system.** An integration of all of the protective measures required to protect an asset against the range of threats applicable to the asset.

**Proximity sensor.** An intrusion detection sensor that changes state based on the close distance or contact of a human to the sensor. These sensors often measure the change in capacitance as a human body enters the measured field.

**Public Information Officer (PIO).** A federal, state, or local government official responsible for preparing and coordinating the dissemination of emergency public information.

## R

**Radiation.** High-energy particles or gamma rays that are emitted by an atom as the substance undergoes radioactive decay. Particles can be either charged alpha or beta particles or neutral neutron or gamma rays.

**Radiation sickness.** The symptoms characterizing the sickness known as radiation injury, resulting from excessive exposure of the whole body to ionizing radiation.

**Radiological monitoring.** The process of locating and measuring radiation by means of survey instruments that can detect and measure (as exposure rates) ionizing radiation.

**Recovery.** The long-term activities beyond the initial crisis period and emergency response phase of disaster operations that focus on returning all systems in the community to a normal status or to reconstitute these systems to a new condition that is less vulnerable.

**Regional Operations Center (ROC).** The temporary operations facility for the coordination of federal response and recovery activities located at the FEMA Regional Office (or Federal

Regional Center) and led by the FEMA Regional Director or Deputy Director until the DFO becomes operational. After the ERT-A is deployed, the ROC performs a support role for federal staff at the disaster scene.

**Report printers.** A separate, dedicated printer attached to the Electronic Security Systems used for generating reports utilizing information stored by the central computer.

**Request-to-exit device.** Passive infrared motion sensors or push buttons that are used to signal an Electronic Entry Control System that egress is imminent or to unlock a door.

**Resolution.** The level to which video details can be determined in a CCTV scene is referred to as resolving ability or resolution.

**Resource Management.** Those actions taken by a government to: identify sources and obtain resources needed to support disaster response activities; coordinate the supply, allocation, distribution, and delivery of resources so that they arrive where and when most needed; and maintain accountability for the resources used.

**Response.** Executing the plan and resources identified to perform those duties and services to preserve and protect life and property as well as provide services to the surviving population.

**Response force.** The people who respond to an act of aggression. Depending on the nature of the threat, the response force could consist of guards, special reaction teams, military or civilian police, an explosives ordnance disposal team, or a fire department.

**Response time.** The length of time from the instant an attack is detected to the instant a security force arrives on site.

**Restricted area.** Any area with access controls that is subject to these special restrictions or controls for security reasons. See controlled area, limited area, exclusion area, and exclusion zone.

**Retinal pattern.** A biometric technology that is based on features of the human eye.

**RF data transmission.** A communications link using radio frequency to send or receive data.

**Risk.** The potential for loss of, or damage to, an asset. It is measured based upon the value of the asset in relation to the threats and vulnerabilities associated with it.

**Rotating drum or rotating plate vehicle barrier.** An active vehicle barrier used at vehicle entrances to controlled areas based on a drum or plate rotating into the path of the vehicle when signaled.

**Routinely occupied.** For the purposes of these standards, an established or predictable pattern of activity within a building that terrorists could recognize and exploit.

**RS-232 data.** IEEE Recommended Standard 232; a point-to-point serial data protocol with a maximum effective distance of 50 feet.

**RS-422 data.** IEEE Recommended Standard 422; a point-to-point serial data protocol with a maximum effective distance of 4,000 feet.

**RS-485 data.** IEEE Recommended Standard 485; a multi-drop serial data protocol with a maximum effective distance of 4,000 feet.

## S

**Sacrificial roof or wall.** Roofs or walls that can be lost in a blast without damage to the primary asset.

**Safe haven.** Secure areas within the interior of the facility. A safe haven should be designed such that it requires more time to penetrate by aggressors than it takes for the response force to reach the protected area to rescue the occupants. It may be a haven from a physical attack or air-isolated haven from CBR contamination.

**Scramble keypad.** A keypad that uses keys on which the numbers change pattern with each use to enhance security by preventing eavesdropping observation of the entered numbers.

**Secondary asset.** An asset that supports a primary asset and whose compromise would indirectly affect the operation of the primary asset.

**Secondary hazard.** A threat whose potential would be realized as the result of a triggering event that of itself would constitute an emergency (e.g., dam failure might be a secondary hazard associated with earthquakes).

**Secure/access mode.** The state of an area monitored by an intrusion detection system in regards to how alarm conditions are reported.

**Security analysis.** The method of studying the nature of and the relationship between assets, threats, and vulnerabilities.

**Security console.** Specialized furniture, racking, and related apparatus used to house the security equipment required in a control center.

**Security engineering.** The process of identifying practical, risk managed short- and long-term solutions to reduce and/or mitigate dynamic manmade hazards by integrating multiple factors, including construction, equipment, manpower, and procedures.

**Security engineering design process.** The process through which assets requiring protection are identified, the threat to and vulnerability of those assets is determined, and a protective system is designed to protect the assets.

**Security Management System database.** In a Security Management System, a database that is transferred to various nodes or panels throughout the system for faster data processing and protection against communications link downtime.

**Security Management System distributed processing.** In a Security Management System, a method of data processing at various

nodes or panels throughout the system for faster data processing and protection against communications links downtime.

**Segregation of duties.** Policies, procedures, and an organizational structure established so that one individual cannot control key aspects of physical and/or computer-related operations and thereby conduct unauthorized actions or gain unauthorized access to minimum essential infrastructure resource elements.

**Semi-isolated fenced perimeters.** Fence lines where approach areas are clear of obstruction for 60 to 100 feet outside of the fence and where the general public or other personnel seldom have reason to be in the area.

**Senior FEMA Official (SFO).** The official appointed by the Director of FEMA, or his representative, that is responsible for deploying to the JOC to serve as the senior interagency consequence management representative on the Command Group, and to manage and coordinate activities taken by the Consequence Management Group.

**Serial interface.** An integration strategy for data transfer where components are connected in series.

**Shielded wire.** Wire with a conductive wrap used to mitigate electromagnetic emanations.

**Situational crime prevention.** A crime prevention strategy based on reducing the opportunities for crime by increasing the effort required to commit a crime, increasing the risks associated with committing the crime, and reducing the target appeal or vulnerability (whether property or person). This opportunity reduction is achieved by management and use policies such as procedures and training, as well as physical approaches such as alteration of the built environment.

**Smart card.** A newer card technology that allows data to be written, stored, and read on a card typically used for identification and/or access.

**Software level integration.** An integration strategy that uses software to interface systems. An example of this would be digital



video displayed in the same computer application window and linked to events of a security management system.

**Specific threat.** Known or postulated aggressor activity focused on targeting a particular asset.

**Stand-off distance.** A distance maintained between a building or portion thereof and the potential location for an explosive detonation or other threat.

**Stand-off weapons.** Weapons such as anti-tank weapons and mortars that are launched from a distance at a target.

**State Coordinating Officer (SCO).** The person appointed by the Governor to coordinate state, commonwealth, or territorial response and recovery activities with FRP-related activities of the Federal Government, in cooperation with the FCO.

**State Liaison.** A FEMA official assigned to a particular state, who handles initial coordination with the state in the early stages of an emergency.

**Stationary vehicle bomb.** An explosive-laden car or truck stopped or parked near a building.

**Storm surge.** A dome of sea water created by the strong winds and low barometric pressure in a hurricane that causes severe coastal flooding as the hurricane strikes land.

**Strain sensitive cable.** Strain sensitive cables are transducers that are uniformly sensitive along their entire length and generate an analog voltage when subjected to mechanical distortions or stress resulting from fence motion. They are typically attached to a chain-link fence about halfway between the bottom and top of the fence fabric with plastic ties.

**Structural protective barriers.** Manmade devices (e.g., fences, walls, floors, roofs, grills, bars, roadblocks, signs, or other construction) used to restrict, channel, or impede access.

**Superstructure.** The supporting elements of a building above the foundation.

**Supplies-bomb delivery.** Bombs or incendiary devices concealed and delivered to supply or material handling points such as loading docks.

**System events.** Events that occur normally in the operation of a security management system. Examples include access control operations and changes of state in intrusion detection sensors.

**System software.** Controls that limit and monitor access to the powerful programs and sensitive files that control the computer hardware and secure applications supported by the system.

## T

**Tactics.** The specific methods of achieving the aggressor's goals to injure personnel, destroy assets, or steal materiel or information.

**Tamper switch.** Intrusion detection sensor that monitors an equipment enclosure for breach.

**Tangle-foot wire.** Barbed wire or tape suspended on short metal or wooden pickets outside a perimeter fence to create an obstacle to approach.

**Taut wire sensor.** An intrusion detection sensor utilizing a column of uniformly spaced horizontal wires, securely anchored at each end and stretched taut. Each wire is attached to a sensor to indicate movement of the wire.

**Technical assistance.** The provisioning of direct assistance to states and local jurisdictions to improve capabilities for program development, planning, and operational performances related to responses to WMD terrorist incidents.

**Technological hazards.** Incidents that can arise from human activities such as manufacture, transportation, storage, and use of hazardous materials. For the sake of simplicity, it is assumed that technological emergencies are accidental and that their consequences are unintended.

**TEMPEST.** An unclassified short name referring to investigations and studies of compromising emanations. It is sometimes used synonymously for the term “compromising emanations” (e.g., TEMPEST tests, TEMPEST inspections).

**Terrorism.** The unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.

**Thermally tempered glass (TTG).** Glass that is heat-treated to have a higher tensile strength and resistance to blast pressures, although with a greater susceptibility to airborne debris.

**Threat.** Any indication, circumstance, or event with the potential to cause loss of, or damage to an asset.

**Threat analysis.** A continual process of compiling and examining all available information concerning potential threats and human-caused hazards. A common method to evaluate terrorist groups is to review the factors of existence, capability, intentions, history, and targeting.

**Time/date stamp.** Data inserted into a CCTV video signal with the time and date of the video as it was created.

**TNT equivalent weight.** The weight of TNT (trinitrotoluene) that has an equivalent energetic output to that of a different weight of another explosive compound.

**Tornado.** A local atmospheric storm, generally of short duration, formed by winds rotating at very high speeds, usually in a counter-clockwise direction. The vortex, up to several hundred yards wide, is visible to the observer as a whirlpool-like column of winds rotating about a hollow cavity or funnel. Winds may reach 300 miles per hour or higher.

**Toxic-free area.** An area within a facility in which the air supply is free of toxic chemical or biological agents.

**Toxicity.** A measure of the harmful effects produced by a given amount of a toxin on a living organism.

**Triple-standard concertina (TSC) wire.** This type of fence uses three rolls of stacked concertina. One roll will be stacked on top of two other rolls that run parallel to each other while resting on the ground, forming a pyramid.

**Tsunami.** Sea waves produced by an undersea earthquake. Such sea waves can reach a height of 80 feet and can devastate coastal cities and low-lying coastal areas.

**Twisted pair wire.** Wire that uses pairs of wires twisted together to mitigate electromagnetic interference.

**Two-person rule.** A security strategy that requires two people to be present in or gain access to a secured area to prevent unobserved access by any individual.

## U

**Unobstructed space.** Space around an inhabited building without obstruction large enough to conceal explosive devices 150 mm (6 inches) or greater in height.

**Unshielded wire.** Wire that does not have a conductive wrap.

## V

**Vault.** A reinforced room for securing items.

**Vertical rod.** Typical door hardware often used with a crash bar to lock a door by inserting rods vertically from the door into the doorframe.

**Vibration sensor.** An intrusion detection sensor that changes state when vibration is present.

**Video intercom system.** An intercom system that also incorporates a small CCTV system for verification.

**Video motion detection.** Motion detection technology that looks for changes in the pixels of a video image.

**Video multiplexer.** A device used to connect multiple video signals to a single location for viewing and/or recording.

**Visual displays.** A display or monitor used to inform the operator visually of the status of the electronic security system.

**Visual surveillance.** The aggressor uses ocular and photographic devices (such as binoculars and cameras with telephoto lenses) to monitor facility or installation operations or to see assets.

**Voice recognition.** A biometric technology that is based on nuances of the human voice.

**Volumetric motion sensor.** An interior intrusion detection sensor that is designed to sense aggressor motion within a protected space.

**Vulnerability.** Any weakness that can be exploited by an aggressor or, in a nonterrorist threat environment, make an asset susceptible to hazard damage.

## W

**Warning.** The alerting of emergency response personnel and the public to the threat of extraordinary danger and the related effects that specific hazards may cause.

**Watch.** Indication in a defined area that conditions are favorable for the specified type of severe weather (e.g., flash flood watch, severe thunderstorm watch, tornado watch, tropical storm watch).

**Waterborne contamination.** Chemical, biological, or radiological agent introduced into and fouling a water supply.

**Weapons-grade material.** Nuclear material considered most suitable for a nuclear weapon. It usually connotes uranium enriched to above 90 percent uranium-235 or plutonium with greater than about 90 percent plutonium-239.

**Weapons of Mass Destruction (WMD).** Any device, material, or substance used in a manner, in a quantity or type, or under circumstances showing an intent to cause death or serious injury to persons, or significant damage to property. An explosive, incendiary, or poison gas, bomb, grenade, rocket having a propellant charge of more than 4 ounces, or a missile having an explosive incendiary charge of more than 0.25 ounce, or mine or device similar to the above; poison gas; weapon involving a disease organism; or weapon that is designed to release radiation or radioactivity at a level dangerous to human life.

**Weigand protocol.** A security industry standard data protocol for card readers.

## Z

**Zoom.** The ability of a CCTV camera to close and focus or open and widen the field of view.

This appendix contains some CBR terms that do not actually appear in this manual. They have been included to present a comprehensive list that pertains to this series of publications.

## **CHEMICAL TERMS**

### **A**

**Acetylcholinesterase.** An enzyme that hydrolyzes the neurotransmitter acetylcholine. The action of this enzyme is inhibited by nerve agents.

**Aerosol.** Fine liquid or solid particles suspended in a gas (e.g., fog or smoke).

**Atropine.** A compound used as an antidote for nerve agents.

### **C**

**Casualty (toxic) agents.** Produce incapacitation, serious injury, or death, and can be used to incapacitate or kill victims. They are the blister, blood, choking, and nerve agents.

**Blister agents.** Substances that cause blistering of the skin. Exposure is through liquid or vapor contact with any exposed tissue (eyes, skin, lungs). Examples are distilled mustard (**HD**), nitrogen mustard (**HN**), lewisite (**L**), mustard/lewisite (**HL**), and phenodichloroarsine (**PD**).

**Blood agents.** Substances that injure a person by interfering with cell respiration (the exchange of oxygen and carbon dioxide between blood and tissues). Examples are arsine (**SA**), cyanogens chloride (**CK**), hydrogen chloride (**HCl**), and hydrogen cyanide (**AC**).

**Choking/lung/pulmonary agents.** Substances that cause physical injury to the lungs. Exposure is through inhalation. In extreme cases, membranes swell and lungs become filled with liquid. Death results from lack of oxygen; hence, the victim is “choked.” Examples are chlorine (**CL**), diphosgene (**DP**), cyanide (**KCN**), nitrogen oxide (**NO**), perfluororisobutylene (**PHIB**), phosgene (**CG**), red phosphorous (**RP**), sulfur trioxide-chlorosulfonic acid (**FS**), Teflon and **PHIB**, titanium tetrachloride (**FM**), and zinc oxide (**HC**).

**Nerve agents.** Substances that interfere with the central nervous system. Exposure is primarily through contact with the liquid (skin and eyes) and secondarily through inhalation of the vapor. Three distinct symptoms associated with nerve agents are: pin-point pupils, an extreme headache, and severe tightness in the chest. See also G-series and V-series nerve agents.

**Chemical agents.** Substances that are intended for use in military operations to kill, seriously injure, or incapacitate people through its physiological effects. Excluded from consideration are riot control agents, and smoke and flame materials. The agent may appear as a vapor, aerosol, or liquid; it can be either a casualty/toxic agent or an incapacitating agent.

**Cutaneous.** Pertaining to the skin.

## D

**Decontamination.** The process of making any person, object, or area safe by absorbing, destroying, neutralizing, making harmless, or removing the hazardous material.





**G-series nerve agents.** Chemical agents of moderate to high toxicity developed in the 1930s. Examples are tabun (**GA**), sarin (**GB**), soman (**GD**), phosphonofluoridic acid, ethyl-, 1-methylethyl ester (**GE**), and cyclohexyl sarin (**GF**).



**Incapacitating agents.** Produce temporary physiological and/or mental effects via action on the central nervous system. Effects may persist for hours or days, but victims usually do not require medical treatment; however, such treatment speeds recovery.

**Vomiting agents.** Produce nausea and vomiting effects; can also cause coughing, sneezing, pain in the nose and throat, nasal discharge, and tears. Examples are adamsite (**DM**), diphenylchloroarsine (**DA**), and diphenylcyanoarsine (**DC**).

**Tear (riot control) agents.** Produce irritating or disabling effects that rapidly disappear within minutes after exposure ceases. Examples are bromobenzylcyanide (**CA**), chloroacetophenone (**CN** or commercially known as Mace), chloropicrin (**PS**), **CNB** (CN in benzene and carbon tetrachloride), **CNC** (CN in chloroform), **CNS** (CN and chloropicrin in chloroform), **CR** (dibenz-(b,f)-1,4-oxazepine, a tear gas), **CS** (tear gas), and **Capsaicin** (pepper spray).

**Central nervous system depressants.** Compounds that have the predominant effect of depressing or blocking the activity of the central nervous system. The primary mental effects include the disruption of the ability to think, sedation, and lack of motivation.

**Central nervous system stimulants.** Compounds that have the predominant effect of flooding the brain with too

much information. The primary mental effect is loss of concentration, causing indecisiveness and the inability to act in a sustained, purposeful manner.

Examples of the depressants and stimulants include agent 15 (suspected Iraqi **BZ**), **BZ** (3-quinulidinyle benzilate), canniboids, fentanyls, **LSD** (lysergic acid diethylamide), and phenothiazines.

**Industrial agents.** Chemicals developed or manufactured for use in industrial operations or research by industry, government, or academia. These chemicals are not primarily manufactured for the specific purpose of producing human casualties or rendering equipment, facilities, or areas dangerous for use by man. Hydrogen cyanide, cyanogen chloride, phosgene, chloropicrin, and many herbicides and pesticides are industrial chemicals that also can be chemical agents.



**Liquid agents.** Chemical agents that appear to be an oily film or droplets. The color ranges from clear to brownish amber.



**Nonpersistent agents.** Agents that, upon release, lose the ability to cause casualties after 10 to 15 minutes. They have a high evaporation rate and are lighter than air and will disperse rapidly. They are considered to be short-term hazards; however, in small unventilated areas, these agents will be more persistent.



**Organophosphorous compound.** A compound containing the elements phosphorus and carbon, whose physiological effects include inhibition of acetylcholinesterase. Many pesticides (malathione and parathion) and virtually all nerve agents are organophosphorous compounds.



**Percutaneous agents.** Agents that are able to be absorbed by the body through the skin.

**Persistent agents.** Agents that, upon release, retain their casualty-producing effects for an extended period of time, usually anywhere from 30 minutes to several days. A persistent agent usually has a low evaporation rate and its vapor is heavier than air. Therefore, its vapor cloud tends to hug the ground. They are considered to be long-term hazards. Although inhalation hazards are still a concern, extreme caution should be taken to avoid skin contact as well.

**Protection.** Any means by which an individual protects his or her body. Measures include masks, self-contained breathing apparatuses, clothing, structures such as buildings, and vehicles.



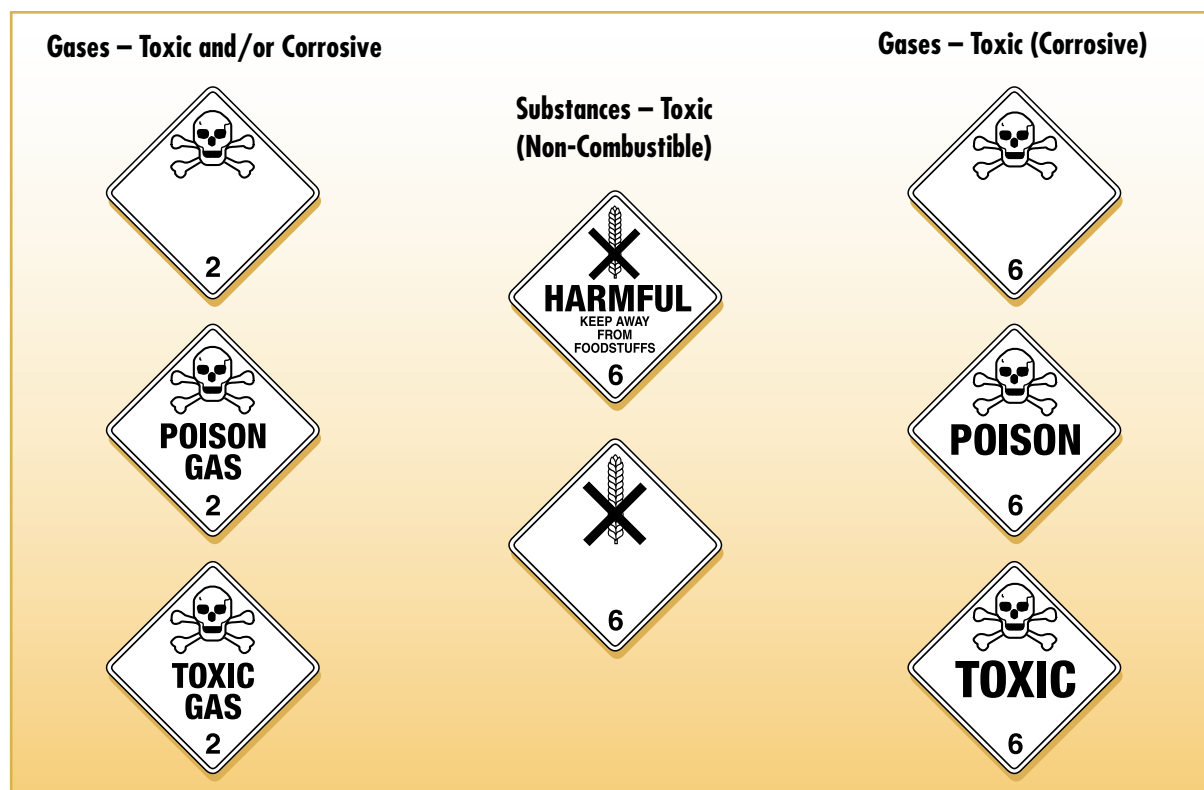
**V-series nerve agents.** Chemical agents of moderate to high toxicity developed in the 1950s. They are generally persistent. Examples are **VE** (phosphonothioic acid, ethyl-, S-[2-(diethylamino)ethyl] O-ethylester), **VG** (phosphorothioic acid, S-[2-(diethylamino)ethyl] O, O-diethyl ester), **VM** (phosphonothioic acid, methyl-, S-[2-(diethylamino)ethyl] O-ethyl ester), **VS** (phosphonothioic acid, ethyl, S-[2-[bis(1-methylethyl)amino]ethyl] O-ethyl

ester), and **VX** (phosphonothioic acid, methyl-, S-[2-[bis(1-methylethyl)amino]ethyl] O-ethyl ester).

**Vapor agents.** A gaseous form of a chemical agent. If heavier than air, the cloud will be close to the ground. If lighter than air, the cloud will rise and disperse more quickly.

**Volatility.** A measure of how readily a substance will vaporize.

### Placards Associated with Chemical Incidents



## BIOLOGICAL TERMS

### A

**Aerosol.** Fine liquid or solid particles suspended in a gas (e.g., fog or smoke).

**Antibiotic.** A substance that inhibits the growth of or kills microorganisms.

**Antisera.** The liquid part of blood containing antibodies that react against disease-causing agents such as those used in biological warfare.

### B

**Bacteria.** Single-celled organisms that multiply by cell division and that can cause disease in humans, plants, or animals.

**Biochemicals.** The chemicals that make up or are produced by living things.

**Biological warfare.** The intentional use of biological agents as weapons to kill or injure humans, animals, or plants, or to damage equipment.

**Biological warfare agents.** Living organisms or the materials derived from them that cause disease in or harm to humans, animals, or plants, or cause deterioration of material. Biological agents may be used as liquid droplets, aerosols, or dry powders.

**Bioregulators.** Biochemicals that regulate bodily functions. Bioregulators that are produced by the body are termed “endogenous.” Some of these same bioregulators can be chemically synthesized.

## C

**Causative agents.** The organism or toxin that is responsible for causing a specific disease or harmful effect.

**Contagious.** Capable of being transmitted from one person to another.

**Culture.** A population of microorganisms grown in a medium.

## D

**Decontamination.** The process of making people, objects, or areas safe by absorbing, destroying, neutralizing, making harmless, or removing the hazardous material.

## F

**Fungi.** Any of a group of plants mainly characterized by the absence of chlorophyll, the green colored compound found in other plants. Fungi range from microscopic single-celled plants (such as molds and mildews) to large plants (such as mushrooms).

## H

**Host.** An animal or plant that harbors or nourishes another organism.

## I

**Incapacitating agents.** Agents that produce physical or psychological effects, or both, that may persist for hours or days after exposure, rendering victims incapable of performing normal physical and mental tasks.

**Infectious agents.** Biological agents capable of causing disease in a susceptible host.

**Infectivity.** (1) The ability of an organism to spread. (2) The number of organisms required to cause an infection to secondary hosts. (3) The capability of an organism to spread out from the site of infection and cause disease in the host organism. Infectivity also can be viewed as the number of organisms required to cause an infection.



**Line-source delivery system.** A delivery system in which the biological agent is dispersed from a moving ground or air vehicle in a line perpendicular to the direction of the prevailing wind. (See also “point-source delivery system.”)



**Microorganism.** Any organism, such as bacteria, viruses, and some fungi, that can be seen only with a microscope.

**Mycotoxin.** A toxin produced by fungi.



**Nebulizer.** A device for producing a fine spray or aerosol.



**Organism.** Any individual living thing, whether animal or plant.

## P

**Parasite.** Any organism that lives in or on another organism without providing benefit in return.

**Pathogen.** Any organism (usually living), such as bacteria, fungi, and viruses, capable of producing serious disease or death.

**Pathogenic agents.** Biological agents capable of causing serious disease.

**Point-source delivery system.** A delivery system in which the biological agent is dispersed from a stationary position. This delivery method results in coverage over a smaller area than with the line-source system. See also line-source delivery system.

## R

**Route of exposure (entry).** The path by which a person comes into contact with an agent or organism (e.g., through breathing, digestion, or skin contact).

## S

**Single-cell protein.** Protein-rich material obtained from cultured algae, fungi, protein, and bacteria, and often used as food or animal feed.

**Spore.** A reproductive form some microorganisms can take to become resistant to environmental conditions, such as extreme heat or cold, while in a “resting stage.”

## T

**Toxicity.** A measure of the harmful effect produced by a given amount of a toxin on a living organism. The relative toxicity of



an agent can be expressed in milligrams of toxin needed per kilogram of body weight to kill experimental animals.

**Toxins.** Poisonous substances produced by living organisms.



**Vaccine.** A preparation of killed or weakened microorganism products used to artificially induce immunity against a disease.

**Vector.** An agent, such as an insect or rat, capable of transferring a pathogen from one organism to another.

**Venom.** A poison produced in the glands of some animals (e.g., snakes, scorpions, or bees).

**Virus.** An infectious microorganism that exists as a particle rather than as a complete cell. Particle sizes range from 20 to 400 nanometers (one-billionth of a meter). Viruses are not capable of reproducing outside of a host cell.

### Placards Associated with Biological Incidents



## RADIOLOGICAL TERMS

### A

**Acute radiation syndrome.** Consists of three levels of effects: hematopoietic (blood cells, most sensitive); gastrointestinal (GI cells, very sensitive); and central nervous system (brain/muscle cells, insensitive). The initial signs and symptoms are nausea, vomiting, fatigue, and loss of appetite. Below about 200 rems, these symptoms may be the only indication of radiation exposure.

**Alpha particles ( $\alpha$ ).** Alpha particles have a very short range in air and a very low ability to penetrate other materials, but also have a strong ability to ionize materials. Alpha particles are unable to penetrate even the thin layer of dead cells of human skin and consequently are not an external radiation hazard. Alpha-emitting nuclides inside the body as a result of inhalation or ingestion are a considerable internal radiation hazard.

### B

**Beta particles ( $\beta$ ).** High-energy electrons emitted from the nucleus of an atom during radioactive decay. They normally can be stopped by the skin or a very thin sheet of metal.

### C

**Cesium-137 (Cs-137).** A strong gamma ray source and can contaminate property, entailing extensive cleanup. It is commonly used in industrial measurement gauges and for irradiation of material. Its half-life is 30.2 years.

**Cobalt-60 (Co-60).** A strong gamma ray source, and is extensively used as a radiotherapeutic for treating cancer, food and material irradiation, gamma radiography, and industrial measurement gauges. Its half-life is 5.27 years.

**Curie (Ci).** A unit of radioactive decay rate defined as  $3.7 \times 10^{10}$  disintegrations per second.

## D

**Decay.** The process by which an unstable element is changed to another isotope or another element by the spontaneous emission of radiation from its nucleus. This process can be measured by using radiation detectors such as Geiger counters.

**Decontamination.** The process of making people, objects, or areas safe by absorbing, destroying, neutralizing, making harmless, or removing the hazardous material.

**Dose.** A general term for the amount of radiation absorbed over a period of time.

**Dosimeter.** A portable instrument for measuring and registering the total accumulated dose to ionizing radiation.

## G

**Gamma ray ( $\gamma$ ).** A high-energy photon emitted from the nucleus of atoms; similar to an x-ray. It can penetrate deeply into body tissue and many materials. Cobalt-60 and Cesium-137 are both strong gamma-emitters. Shielding against gamma radiation requires thick layers of dense materials, such as lead. Gamma rays are potentially lethal to humans.

## H

**Half-life.** The amount of time needed for half of the atoms of a radioactive material to decay.

**Highly enriched uranium (HEU).** Uranium that is enriched to above 20 percent Uranium-235 (U-235). Weapons-grade HEU is enriched to above 90 percent in U-235.

**Ionize.** To split off one or more electrons from an atom, thus leaving it with a positive electric charge. The electrons usually attach to one of the atoms or molecules, giving them a negative charge.

**Iridium-192.** A gamma ray emitting radioisotope used for gamma radiography. Its half-life is 73.83 days.

**Isotope.** A specific element always has the same number of protons in the nucleus. That same element may, however, appear in forms that have different numbers of neutrons in the nucleus. These different forms are referred to as “isotopes” of the element; for example, deuterium (**2H**) and tritium (**3H**) are isotopes of ordinary hydrogen (**H**).

**Lethal dose (50/30).** The dose of radiation expected to cause death within 30 days to 50 percent of those exposed without medical treatment. The generally accepted range is from 400-500 rem received over a short period of time.

**Nuclear reactor.** A device in which a controlled, self-sustaining nuclear chain reaction can be maintained with the use of cooling to remove generated heat.

## P

**Plutonium-239 (Pu-239).** A metallic element used for nuclear weapons. Its half-life is 24,110 years.

## R

**Rad.** A unit of absorbed dose of radiation defined as deposition of 100 ergs of energy per gram of tissue. A rad amounts to approximately one ionization per cubic micron.

**Radiation.** High energy alpha or beta particles or gamma rays that are emitted by an atom as the substance undergoes radioactive decay.

**Radiation sickness.** Symptoms resulting from excessive exposure to radiation of the body.

**Radioactive waste.** Disposable, radioactive materials resulting from nuclear operations. Wastes are generally classified into two categories, high-level and low-level.

**Radiological Dispersal Device (RDD).** A device (weapon or equipment), other than a nuclear explosive device, designed to disseminate radioactive material in order to cause destruction, damage, or injury by means of the radiation produced by the decay of such material.

**Radioluminescence.** The luminescence produced by particles emitted during radioactive decay.

**Roentgen Equivalent Man (REM or rem).** A unit of absorbed dose that takes into account the relative effectiveness of radiation that harms human health.

## S

**Shielding.** Materials (lead, concrete, etc.) used to block or attenuate radiation for protection of equipment, materials, or people.

**Special Nuclear Material (SNM).** Plutonium and uranium enriched in the isotopes Uranium-233 or Uranium-235.

## U

**Uranium 235 (U-235).** Naturally-occurring U-235 is found at 0.72 percent enrichment. U-235 is used as a reactor fuel or for weapons; however, weapons typically use U-235 enriched to 90 percent. Its half-life is  $7.04 \times 10^8$  years.

## X

**X-ray.** An invisible, highly penetrating electromagnetic radiation of much shorter wavelength (higher frequency) than visible light. Very similar to gamma rays.

### Placards Associated with Radiological Incidents



The following web sites are available for further clarification or for terms not used in this manual:

Chemical, Biological, Radiological (CBR)  
[Formerly NBC (Nuclear, Biological, Chemical)]

<http://www.nbc-med.org/SiteContent/glossary.asp?B>

<http://www.nbcprotect.com/new/glossary.htm>

C-17

Sources:

U.S. Department of the Army, *Potential Military Chemical/Biological Agents and Compounds*, U.S. Army Field Manual 3-9, (NAVFAC P-467, AFR 355-7), 12 December 1990. Washington, D.C.: U.S. Government Printing Office.

Committee on Toxicology, National Research Council. 1997. *Review of Acute Human Toxicity Estimates for Selected Chemical Warfare Agents*. Washington, D.C.: National Academy Press.

Tables reduced for review purposes only. These tables will be appear as 11x17 foldout pages in the printed publication.





# SELECTED BIOLOGICAL AGENT CHARACTERISTICS

Agent Type	Disease/Condition and Pathogen	Description of Agent	Transmissibility and Prevalence	Infectivity and Latency	Incubation Period	Duration of Illness	Permeability/ Stability	Vaccination/ Treatment	Signs and Symptoms	Treatment	Possible Means of Delivery
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z	Anthrax (Bacillus anthracis)	Spore-forming, gram-positive, aerobic, rod-shaped bacteria (1-10 µm x 2-5 µm). Spores are highly resistant to heat and chemicals.	No	High/Low	1-10 days	1-10 days	Stable in soil for decades	Yes	Fever, malaise, fatigue, cough and mild chest discomfort, followed by severe respiratory distress. Skin lesions (papules, vesicles, ulcers) may develop. Gastrointestinal symptoms (nausea, vomiting, diarrhea) may occur.	Antibiotics (penicillin or fluoroquinolones) and supportive care. Anthrax vaccine (Anthrax Vaccine Adsorbed) is available for pre-exposure prophylaxis.	Aerosol (inhalation), Contaminated food or water (ingestion), Spores in soil (cutaneous)
	Breast Cancer (various agents)	Not a biological agent, but a common disease.	No	High/Low	Months to years	Months to years	Stable in soil for decades	Yes	Swelling, pain, redness, and changes in the breast tissue. Lymph node enlargement may occur.	Chemotherapy, hormone therapy, surgery, and radiation therapy.	Contaminated food or water (ingestion), Spores in soil (cutaneous)
	Cholera (Vibrio cholerae)	Gram-negative, comma-shaped, non-spore-forming bacteria. Produces a potent enterotoxin.	High	High/Low	1-5 days	1-5 days	Stable in water for weeks	Yes	Watery, rice-water stool, severe dehydration, muscle cramps, and rapid heart rate.	Oral rehydration therapy (ORT) and antibiotics (tetracycline or fluoroquinolones).	Contaminated food or water (ingestion)
	Coccidia (various species)	Parasitic protozoans that infect the intestines of various animals, including humans.	High	High/Low	1-10 days	1-10 days	Stable in soil for weeks	Yes	Diarrhea, abdominal pain, and weight loss.	Antibiotics (trimethoprim-sulfamethoxazole) and supportive care.	Contaminated food or water (ingestion)
	Diphtheria (Corynebacterium diphtheriae)	Gram-positive, rod-shaped, non-spore-forming bacteria. Produces a potent exotoxin.	High	High/Low	1-10 days	1-10 days	Stable in soil for weeks	Yes	Sore throat, fever, and a thick, white membrane in the throat.	Antitoxin and antibiotics (penicillin or erythromycin).	Contaminated food or water (ingestion)
	Ebola (Ebola virus)	Single-stranded, enveloped, negative-sense RNA virus. Causes severe hemorrhagic fever.	High	High/Low	2-16 days	2-16 days	Stable in blood for weeks	Yes	Fever, fatigue, muscle aches, and bleeding from various sites.	Supportive care and experimental treatments.	Contaminated blood or body fluids (contact), Contaminated needles (injection)
	Flu (Influenza virus)	Single-stranded, enveloped, negative-sense RNA virus. Causes respiratory illness.	High	High/Low	1-4 days	1-4 days	Stable in air for hours	Yes	Fever, cough, sore throat, and fatigue.	Antiviral drugs (oseltamivir) and supportive care.	Aerosol (inhalation)
	Hepatitis (various viruses)	Group of viruses that cause inflammation of the liver. Includes Hepatitis A, B, C, D, and E.	High	High/Low	1-6 weeks	1-6 weeks	Stable in blood for years	Yes	Jaundice, fatigue, and abdominal pain.	Supportive care and antiviral drugs (for Hepatitis B and C).	Contaminated blood or body fluids (contact), Contaminated needles (injection)
	Measles (Measles virus)	Single-stranded, enveloped, negative-sense RNA virus. Causes a highly contagious respiratory illness.	High	High/Low	7-14 days	7-14 days	Stable in air for hours	Yes	Fever, cough, and a characteristic red rash.	Vaccine (MMR) and supportive care.	Aerosol (inhalation)
	Mumps (Mumps virus)	Single-stranded, enveloped, negative-sense RNA virus. Causes swelling of the salivary glands.	High	High/Low	1-4 weeks	1-4 weeks	Stable in air for hours	Yes	Swelling of the salivary glands, fever, and headache.	Supportive care and antiviral drugs (experimental).	Aerosol (inhalation)
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z	Botulism (Clostridium botulinum)	Gram-positive, rod-shaped, spore-forming bacteria. Produces a potent neurotoxin.	No	High/Low	1-10 days	1-10 days	Stable in soil for decades	Yes	Blurred vision, drooping eyelids, and muscle paralysis.	Antitoxin and supportive care.	Contaminated food or water (ingestion), Wound (injection)
	Cholera (Vibrio cholerae)	Gram-negative, comma-shaped, non-spore-forming bacteria. Produces a potent enterotoxin.	High	High/Low	1-5 days	1-5 days	Stable in water for weeks	Yes	Watery, rice-water stool, severe dehydration, muscle cramps, and rapid heart rate.	Oral rehydration therapy (ORT) and antibiotics (tetracycline or fluoroquinolones).	Contaminated food or water (ingestion)
	Diphtheria (Corynebacterium diphtheriae)	Gram-positive, rod-shaped, non-spore-forming bacteria. Produces a potent exotoxin.	High	High/Low	1-10 days	1-10 days	Stable in soil for weeks	Yes	Sore throat, fever, and a thick, white membrane in the throat.	Antitoxin and antibiotics (penicillin or erythromycin).	Contaminated food or water (ingestion)
	Ebola (Ebola virus)	Single-stranded, enveloped, negative-sense RNA virus. Causes severe hemorrhagic fever.	High	High/Low	2-16 days	2-16 days	Stable in blood for weeks	Yes	Fever, fatigue, muscle aches, and bleeding from various sites.	Supportive care and experimental treatments.	Contaminated blood or body fluids (contact), Contaminated needles (injection)
	Flu (Influenza virus)	Single-stranded, enveloped, negative-sense RNA virus. Causes respiratory illness.	High	High/Low	1-4 days	1-4 days	Stable in air for hours	Yes	Fever, cough, sore throat, and fatigue.	Antiviral drugs (oseltamivir) and supportive care.	Aerosol (inhalation)
	Hepatitis (various viruses)	Group of viruses that cause inflammation of the liver. Includes Hepatitis A, B, C, D, and E.	High	High/Low	1-6 weeks	1-6 weeks	Stable in blood for years	Yes	Jaundice, fatigue, and abdominal pain.	Supportive care and antiviral drugs (for Hepatitis B and C).	Contaminated blood or body fluids (contact), Contaminated needles (injection)
	Measles (Measles virus)	Single-stranded, enveloped, negative-sense RNA virus. Causes a highly contagious respiratory illness.	High	High/Low	7-14 days	7-14 days	Stable in air for hours	Yes	Fever, cough, and a characteristic red rash.	Vaccine (MMR) and supportive care.	Aerosol (inhalation)
	Mumps (Mumps virus)	Single-stranded, enveloped, negative-sense RNA virus. Causes swelling of the salivary glands.	High	High/Low	1-4 weeks	1-4 weeks	Stable in air for hours	Yes	Swelling of the salivary glands, fever, and headache.	Supportive care and antiviral drugs (experimental).	Aerosol (inhalation)
	Polio (Poliovirus)	Single-stranded, non-enveloped, positive-sense RNA virus. Causes paralysis.	No	High/Low	1-10 days	1-10 days	Stable in air for hours	Yes	Weakness and paralysis of the limbs.	Vaccine (IPV) and supportive care.	Contaminated food or water (ingestion), Contaminated needles (injection)
	Rabies (Rabies virus)	Single-stranded, enveloped, negative-sense RNA virus. Causes a fatal encephalitis.	No	High/Low	1-10 days	1-10 days	Stable in air for hours	Yes	Agitation, hallucinations, and paralysis.	Supportive care and experimental treatments.	Contaminated food or water (ingestion), Contaminated needles (injection)
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z	Botulism (Clostridium botulinum)	Gram-positive, rod-shaped, spore-forming bacteria. Produces a potent neurotoxin.	No	High/Low	1-10 days	1-10 days	Stable in soil for decades	Yes	Blurred vision, drooping eyelids, and muscle paralysis.	Antitoxin and supportive care.	Contaminated food or water (ingestion), Wound (injection)
	Cholera (Vibrio cholerae)	Gram-negative, comma-shaped, non-spore-forming bacteria. Produces a potent enterotoxin.	High	High/Low	1-5 days	1-5 days	Stable in water for weeks	Yes	Watery, rice-water stool, severe dehydration, muscle cramps, and rapid heart rate.	Oral rehydration therapy (ORT) and antibiotics (tetracycline or fluoroquinolones).	Contaminated food or water (ingestion)
	Diphtheria (Corynebacterium diphtheriae)	Gram-positive, rod-shaped, non-spore-forming bacteria. Produces a potent exotoxin.	High	High/Low	1-10 days	1-10 days	Stable in soil for weeks	Yes	Sore throat, fever, and a thick, white membrane in the throat.	Antitoxin and antibiotics (penicillin or erythromycin).	Contaminated food or water (ingestion)
	Ebola (Ebola virus)	Single-stranded, enveloped, negative-sense RNA virus. Causes severe hemorrhagic fever.	High	High/Low	2-16 days	2-16 days	Stable in blood for weeks	Yes	Fever, fatigue, muscle aches, and bleeding from various sites.	Supportive care and experimental treatments.	Contaminated blood or body fluids (contact), Contaminated needles (injection)
	Flu (Influenza virus)	Single-stranded, enveloped, negative-sense RNA virus. Causes respiratory illness.	High	High/Low	1-4 days	1-4 days	Stable in air for hours	Yes	Fever, cough, sore throat, and fatigue.	Antiviral drugs (oseltamivir) and supportive care.	Aerosol (inhalation)
	Hepatitis (various viruses)	Group of viruses that cause inflammation of the liver. Includes Hepatitis A, B, C, D, and E.	High	High/Low	1-6 weeks	1-6 weeks	Stable in blood for years	Yes	Jaundice, fatigue, and abdominal pain.	Supportive care and antiviral drugs (for Hepatitis B and C).	Contaminated blood or body fluids (contact), Contaminated needles (injection)
	Measles (Measles virus)	Single-stranded, enveloped, negative-sense RNA virus. Causes a highly contagious respiratory illness.	High	High/Low	7-14 days	7-14 days	Stable in air for hours	Yes	Fever, cough, and a characteristic red rash.	Vaccine (MMR) and supportive care.	Aerosol (inhalation)
	Mumps (Mumps virus)	Single-stranded, enveloped, negative-sense RNA virus. Causes swelling of the salivary glands.	High	High/Low	1-4 weeks	1-4 weeks	Stable in air for hours	Yes	Swelling of the salivary glands, fever, and headache.	Supportive care and antiviral drugs (experimental).	Aerosol (inhalation)
	Polio (Poliovirus)	Single-stranded, non-enveloped, positive-sense RNA virus. Causes paralysis.	No	High/Low	1-10 days	1-10 days	Stable in air for hours	Yes	Weakness and paralysis of the limbs.	Vaccine (IPV) and supportive care.	Contaminated food or water (ingestion), Contaminated needles (injection)
	Rabies (Rabies virus)	Single-stranded, enveloped, negative-sense RNA virus. Causes a fatal encephalitis.	No	High/Low	1-10 days	1-10 days	Stable in air for hours	Yes	Agitation, hallucinations, and paralysis.	Supportive care and experimental treatments.	Contaminated food or water (ingestion), Contaminated needles (injection)

This appendix contains some CBR terms that do not actually appear in this manual. They have been included to present a comprehensive list that pertains to this series of publications.

## CHEMICAL TERMS

### A

**Acetylcholinesterase.** An enzyme that hydrolyzes the neurotransmitter acetylcholine. The action of this enzyme is inhibited by nerve agents.

**Aerosol.** Fine liquid or solid particles suspended in a gas (e.g., fog or smoke).

**Atropine.** A compound used as an antidote for nerve agents.

### C

**Casualty (toxic) agents.** Produce incapacitation, serious injury, or death, and can be used to incapacitate or kill victims. They are the blister, blood, choking, and nerve agents.

**Blister agents.** Substances that cause blistering of the skin. Exposure is through liquid or vapor contact with any exposed tissue (eyes, skin, lungs). Examples are distilled mustard (**HD**), nitrogen mustard (**HN**), lewisite (**L**), mustard/lewisite (**HL**), and phenodichloroarsine (**PD**).

**Blood agents.** Substances that injure a person by interfering with cell respiration (the exchange of oxygen and carbon dioxide between blood and tissues). Examples are arsine (**SA**), cyanogens chloride (**CK**), hydrogen chloride (**HCl**), and hydrogen cyanide (**AC**).

**Choking/lung/pulmonary agents.** Substances that cause physical injury to the lungs. Exposure is through inhalation. In extreme cases, membranes swell and

**A**n overall site-security system is composed of three major subelements: detection, delay, and response. The detection subelement includes intrusion detection, assessment, and entry control. The purpose of this appendix is to introduce the basic concepts of site security systems, including the use of Electronic Security Systems (ESSs), boundary-penetration sensors, volumetric motion sensors, exterior intrusion detection sensors, microwave sensors, infrared sensors, video motion sensors, electronic entry control, and monitoring designated restricted areas.

## USE OF ESS

An ESS is an integrated system that encompasses interior and exterior sensors; closed circuit television (CCTV) systems for assessing alarm conditions; Electronic Entry Control Systems (EECSs); data-transmission media (DTM); and alarm reporting systems for monitoring, controlling, and displaying various alarm and system information. Interior and exterior sensors and their associated communication and display subsystems are collectively called IDSs.

An ESS is used to provide early warning of an intruder. This system consists of hardware and software elements operated by trained security personnel.

A system is configured to provide one or more layers of detection around an asset. Each layer is made up of a series of contiguous detection zones designed to isolate the asset and to control the entry and exit of authorized personnel and materials.

## General ESS Description

An ESS consists of sensors interfaced with electronic entry control devices, CCTV, alarm reporting displays (both visual and audible), and security lighting. The situation is assessed by sending guards

to the alarm point or by using CCTV. Alarm reporting devices and video monitors are located in the security center. The asset's importance will determine whether multiple or redundant security centers are required and, ultimately, the required sophistication of all elements in the ESS. Digital and analog data are transmitted from local (field) interior and exterior locations to the security center for processing. Reliability and accuracy are important functional requirements of the data-transmission system.

### **ESS Design Considerations**

A facility may require interior and exterior ESS elements, depending on the level of protection required. The applicable regulations, threat, and design criteria will define the ESS's general requirements. For an existing ESS, hardware and software may need to be supplemented, upgraded, or completely replaced. A site layout (in which all assets are identified and located) is required. It is a useful design tool for such tasks as configuring the DTM.

The exterior and interior IDSs should be configured as layers of unbroken rings concentrically surrounding the asset. These rings should correspond to defensive layers that constitute the delay system. The first detection layer is located at the outermost defensive layer necessary to provide the required delay. Detection layers can be on a defensive layer, in the area between two defensive layers, or on the asset itself, depending on the delay required. For example, if a wall of an interior room provides sufficient delay for effective response to aggression, detection layers could be between the facility exterior and interior-room wall or on the interior-room wall. They would detect the intruder before penetration of the interior wall is possible.

### **PERIMETER LAYOUT AND ZONING SENSORS**

A protected area's perimeter is usually defined by an enclosing wall or fence or a natural barrier such as water. For exterior sensors to be effective, the perimeter around which they are to be deployed must be precisely defined. In most applications, a dual

chain-link-fence configuration will be established around the perimeter (see Chapter 2.4.1 for additional information). Typically, fences should be between 30 and 50 feet apart; as the distance increases, it is harder for an intruder to bridge the fences. If fence separation is less than 30 feet, some microwave and ported coax sensors cannot be used. The area between fences (called the controlled area or isolation zone) may need to be cleared of vegetation and graded, depending on the type of sensor used. Proper drainage is required to preclude standing water and to prevent the formation of gullies caused by running water after a heavy rain or melting snow. Cleared areas are required inside and outside of the controlled area. These areas enhance routine observation, as well as sensor-alarm assessment, and minimize the protective cover available to a would-be intruder.

After the perimeter has been defined, the next step is to divide it into specific detection zones. The length of each detection zone is determined by evaluating the contour, the existing terrain, and the operational activities along the perimeter. Detection zones should be long and straight to minimize the number of sensors or cameras necessary and to aid guard assessment if cameras are not used. It may be more economical to straighten an existing fence line than to create numerous detection zones in accommodating a crooked fence line. If the perimeter is hilly and line of sight (LOS) sensors or CCTV assessment are used, the length of individual detection zones will be commensurate with sensor limitations. Entry points for personnel and vehicles must be configured as independent zones. This enables deactivation of the sensors in these zones; that is, placing them in the access mode during customary working hours (assuming the entry points are manned) without having to deactivate adjacent areas.

The specific length of individual zones can vary around the perimeter. Although specific manufacturers may advertise maximum zone lengths exceeding 1,000 feet, it is not practical to exceed a zone length of 300 feet. If the zone is longer, it will be difficult for an operator using CCTV assessment or for the response force to identify the location of an intrusion or the cause of a false alarm.

When establishing zones using multiple sensors, the designer should establish coincident zones where the length and location of each individual sensor will be identical for all sensors within a given zone. If an alarm occurs in a specific zone, the operator can readily determine its approximate location by referring to a map of the perimeter. This also minimizes the number of CCTV cameras required for assessment and simplifies the interface between the alarm-annunciation system and the CCTV switching system.

## BOUNDARY-PENETRATION SENSORS

Boundary-penetration sensors are designed to detect penetration or attempted penetration through perimeter barriers. These barriers include walls, ceilings, duct openings, doors, and windows.

- **Structural-vibration sensors.** Structural-vibration sensors detect low-frequency energy generated in an attempted penetration of a physical barrier (such as a wall or a ceiling) by hammering, drilling, cutting, detonating explosives, or employing other forcible methods of entry. A piezoelectric transducer senses mechanical energy and converts it into electrical signals proportional in magnitude to the vibrations.
- **Glass-breakage sensors.** Glass-breakage sensors detect the breaking of glass. The noise from breaking glass consists of frequencies in both the audible and ultrasonic range. Glass-breakage sensors use microphone transducers to detect the glass breakage. The sensors are designed to respond to specific frequencies only, thus minimizing such false alarms as may be caused by banging on the glass.
- **Passive ultrasonic sensors.** Passive ultrasonic sensors detect acoustical energy in the ultrasonic frequency range, typically between 20 and 30 kilohertz (kHz). They are used to detect an attempted penetration through rigid barriers (such as metal or masonry walls, ceilings, and floors). They also detect penetration through windows and vents covered by metal grilles, shutters, or bars if these openings are properly sealed against outside sounds.

- **Balanced magnetic switches.** Balanced magnetic switches (BMSs) are typically used to detect the opening of a door. These sensors can also be used on windows, hatches, gates, or other structural devices that can be opened to gain entry. When using a BMS, mount the switch mechanism on the doorframe and the actuating magnet on the door. Typically, the BMS has a three-position reed switch and an additional magnet (called the bias magnet) located adjacent to the switch. When the door is closed, the reed switch is held in the balanced or center position by interacting magnetic fields. If the door is opened or an external magnet is brought near the sensor in an attempt to defeat it, the switch becomes unbalanced and generates an alarm. A BMS must be mounted so that the magnet receives maximum movement when the door or window is opened.
- **Grid wire sensors.** The grid wire sensor consists of a continuous electrical wire arranged in a grid pattern. The wire maintains an electrical current. An alarm is generated when the wire is broken. The sensor detects forced entry through walls, floors, ceilings, doors, windows, and other barriers. An enamel-coated number 24 or 26 American wire gauge (AWG) solid-copper wire typically forms the grid. The grid's maximum size is determined by the spacing between the wires, the wire's resistance, and the electrical characteristics of the source providing the current. The grid wire can be installed directly on the barrier, in a grille or screen that is mounted on the barrier, or over an opening that requires protection.

## **VOLUMETRIC MOTION SENSORS**

Volumetric motion sensors are designed to detect intruder motion within the interior of a protected volume. Volumetric sensors may be active or passive. Active sensors (such as microwave) fill the volume to be protected with an energy pattern and recognize a disturbance in the pattern when anything moves within the detection zone. Whereas active sensors generate their own energy pattern to detect an intruder, passive sensors (such as infrared



(IR)) detect energy generated by an intruder. Some sensors, known as dual technology sensors, use a combination of two different technologies, usually one active and one passive, within the same unit. If CCTV assessment or surveillance cameras are installed, video motion sensors can be used to detect intruder movement within the area. Because ultrasonic motion sensors are seldom used, they will not be discussed herein.

- **Microwave motion sensors.** With microwave motion sensors, high-frequency electromagnetic energy is used to detect an intruder's motion within the protected area. Interior or sophisticated microwave motion sensors are normally used.
  - **Interior microwave motion sensors.** Interior microwave motion sensors are typically monostatic; the transmitter and the receiver are housed in the same enclosure (transceiver).
  - **Sophisticated microwave motion sensors.** Sophisticated microwave motion sensors may be equipped with electronic range gating. This feature allows the sensor to ignore the signals reflected beyond the settable detection range. Range gating may be used to effectively minimize unwanted alarms from activity outside the protected area.
- **Passive infrared (PIR) motion sensors.** PIR motion sensors detect a change in the thermal energy pattern caused by a moving intruder and initiate an alarm when the change in energy satisfies the detector's alarm criteria. These sensors are passive devices because they do not transmit energy; they monitor the energy radiated by the surrounding environment.
- **Dual technology sensors.** To minimize the generation of alarms caused by sources other than intruders, dual-technology sensors combine two different technologies in one unit. Ideally, this is achieved by combining two sensors that individually have a high probability of detection (POD) and do not respond to common sources of false alarms. Available dual-



technology sensors combine an active ultrasonic or microwave sensor with a PIR sensor. The alarms from each sensor are logically combined in an “and” configuration (i.e., nearly simultaneous alarms from both active and passive sensors are needed to produce a valid alarm).

- **Video motion sensors.** A video motion sensor generates an alarm when an intruder enters a selected portion of a CCTV camera’s field of view. The sensor processes and compares successive images between the images against predefined alarm criteria. There are two categories of video motion detectors, analog and digital. Analog detectors generate an alarm in response to changes in a picture’s contrast. Digital devices convert selected portions of the analog video signal into digital data that are compared with data converted previously; if differences exceed preset limits, an alarm is generated. The signal processor usually provides an adjustable window that can be positioned anywhere on the video image. Available adjustments permit changing horizontal and vertical window size, window position, and window sensitivity. More sophisticated units provide several adjustable windows that can be individually sized and positioned. Multiple windows permit concentrating on several specific areas of an image while ignoring others. For example, in a scene containing six doorways leading into a long hallway, the sensor can be set to monitor only two critical doorways.
- **Point sensors.** Point sensors are used to protect specific objects within a facility. These sensors (sometimes referred to as proximity sensors) detect an intruder coming in close proximity to, touching, or lifting an object. Several different types are available, including capacitance sensors, pressure mats, and pressure switches. Other types of sensors can also be used for object protection.
- **Capacitance sensors.** Capacitance sensors detect an intruder approaching or touching a metal object by sensing a change in capacitance between the object and the ground. A capacitor

consists of two metallic plates separated by a dielectric medium. A change in the dielectric medium or electrical charge results in a change in capacitance. In practice, the metal object to be protected forms one plate of the capacitor and the ground plane surrounding the object forms the second plate. The sensor processor measures the capacitance between the metal object and the ground plane. An approaching intruder alters the dielectric value, thus changing the capacitance. If the net capacitance change satisfies the alarm criteria, an alarm is generated.

- **Pressure mats.** Pressure mats generate an alarm when pressure is applied to any part of the mat's surface, such as when someone steps on the mat. One type of construction uses two layers of copper screening separated by soft-sponge rubber insulation with large holes in it. Another type uses parallel strips of ribbon switches made from two strips of metal separated by an insulating material and spaced several inches apart. When enough pressure is applied to the mat, either the screening or the metal strips make contact, generating an alarm. Pressure mats can be used to detect an intruder approaching a protected object, or they can be placed by doors or windows to detect entry. Because pressure mats are easy to bridge, they should be well concealed, such as placing them under a carpet.
- **Pressure switches.** Mechanically activated contact switches or single ribbon switches can be used as pressure switches. Objects that require protection can be placed on top of the switch. When the object is moved, the switch actuates and generates an alarm. In this usage, the switch must be well concealed. The interface between the switch and the protected object should be designed so that an adversary cannot slide a thin piece of material under the object to override the switch while the object is removed.

## EXTERIOR INTRUSION DETECTION SENSORS

Exterior intrusion detection sensors are customarily used to detect an intruder crossing the boundary of a protected area. They can also be used in clear zones between fences or around buildings, for protecting materials and equipment stored outdoors within a protected boundary, or in estimating the POD for buildings and other facilities.

Because of the nature of the outdoor environment, exterior sensors are also more susceptible to nuisance and environmental alarms than interior sensors. Inclement weather conditions (e.g., heavy rain, hail, and high wind), vegetation, the natural variation of the temperature of objects in the detection zone, blowing debris, and animals are major sources of unwanted alarms.

Due to this vulnerability, it is extremely important that enclosures are located and installed properly and that adequate physical protection is provided. Several different types of exterior intrusion detection sensors are available:

- Fence sensors
- Buried line sensors
- Video motion sensors

## FENCE SENSORS

Fence sensors detect attempts to penetrate a fence around a protected area. Penetration attempts (e.g., climbing, cutting, or lifting) generate mechanical vibrations and stresses in fence fabric and posts that are usually different than those caused by natural phenomena like wind and rain. The basic types of sensors used to detect these vibrations and stresses are strain sensitive cable, taut wire, fiber optics, and capacitance.

- **Strain sensitive cables.** Strain sensitive cables are transducers that are uniformly sensitive along their entire length. They generate an analog voltage when subject to mechanical

distortions or stress resulting from fence motion. Strain sensitive cables are sensitive to both low and high frequencies. Because the cable acts like a microphone, some manufacturers offer an option that allows the operator to listen to fence noises causing the alarm. Operators can then determine whether the noises are naturally occurring sounds from wind or rain or are from an actual intrusion attempt.

- **Taut wire sensors.** Taut wire sensors combine a physically taut-wire barrier with an intrusion detection sensor network. The taut wire sensor consists of a column of uniformly spaced horizontal wires up to several hundred feet in length and securely anchored at each end. Typically, the wires are spaced 4 to 8 inches apart. Each is individually tensioned and attached to a detector located in a sensor post. Two types of detectors are commonly used, mechanical switches and strain gauges.
- **Fiber optic cable sensors.** Fiber optic cable sensors are functionally equivalent to the strain-sensitive cable sensors previously discussed. However, rather than electrical signals, modulated light is transmitted down the cable and the resulting received signals are processed to determine whether an alarm should be initiated. Because the cable contains no metal and no electrical signal is present, fiber optic sensors are generally less susceptible to electrical interference from lightning or other sources.
- **Capacitance proximity sensors.** Capacitance proximity sensors measure the electrical capacitance between the ground and an array of sense wires. Any variations in capacitance, such as that caused by an intruder approaching or touching one of the sense wires, initiates an alarm. These sensors usually consist of two or three wires attached to outriggers along the top of an existing fence, wall, or roof edge.

## **BURIED LINE SENSORS**

A buried line sensor system consists of detection probes or cable buried in the ground, typically between two fences that form an

isolation zone. These devices are wired to an electronic processing unit. The processing unit generates an alarm if an intruder passes through the detection field. Buried line sensors have several significant features:

- They are hidden, making them difficult to detect and circumvent.
- They follow the terrain's natural contour.
- They do not physically interfere with human activity, such as grass mowing or snow removal.
- They are affected by certain environmental conditions, such as running water and ground freeze/thaw cycles. (Seismic, seismic/magnetic, magnetic, and balanced pressure sensors are seldom used and will not be discussed herein.)

## **MICROWAVE SENSORS**

Microwave intrusion detection sensors are categorized as bistatic or monostatic. Bistatic sensors use transmitting and receiving antennas located at opposite ends of the microwave link, whereas monostatic sensors use the same antenna.

- A bistatic system uses a transmitter and a receiver that are typically separated by 100 to 1,200 feet and that are within direct LOS of each other.
- Monostatic microwave sensors use the same antenna or virtually coincident antenna arrays for the transmitter and receiver, which are usually combined into a single package.

## **INFRARED (IR) SENSORS**

The IR sensors are available in both active and passive models. An active sensor generates one or more near-IR beams that generate an alarm when interrupted. A passive sensor detects changes in thermal IR radiation from objects located within its field of view.

Active sensors consist of transmitter/receiver pairs. The transmitter contains an IR light source (such as a gallium arsenide light-emitting diode [LED]) that generates an IR beam. The light source is usually modulated to reduce the sensor's susceptibility to unwanted alarms resulting from sunlight or other IR light sources. The receiver detects changes in the signal power of the received beam. To minimize nuisance alarms from birds or blowing debris, the alarm criteria usually require that a high percentage of the beam be blocked for a specific interval of time.

## **VIDEO MOTION SENSORS**

Video motion sensors are available on most digital video recorders used in security applications. They can be programmed to activate alarms, initiate recording, or any other designated action when motion is detected by a security camera. Some digital video recorders can be programmed to monitor very specific fields of view for specific rates of motion in order to increase effectiveness and minimize extraneous detections. Video motion sensors can also greatly improve the efficiency of security personnel monitoring security cameras by alerting them when motion is detected.

## **ELECTRONIC ENTRY CONTROL**

The function of an entry control system is to ensure that only authorized personnel are permitted into or out of a controlled area. Entry can be controlled by locked fence gates, locked doors to a building or rooms within a building, or specially designed portals.

These means of entry control can be applied manually by guards or automatically by using entry control devices. In a manual system, guards verify that a person is authorized to enter an area, usually by comparing the photograph and personal characteristics of the individual requesting entry. In an automated system, the entry control device verifies that a person is authorized to enter or exit. The automated system usually interfaces with locking mechanisms on doors or gates that open momentarily to permit passage.

Mechanical hardware (e.g., locking mechanisms, electric door strikes, and specially designed portal hardware) and equipment used to detect contraband material (e.g., metal detectors, X-ray baggage-search systems, explosives detectors, and special nuclear-material monitors) are described in other documentation.

All entry control systems control passage by using one or more of three basic techniques (e.g., something a person knows, something a person has, or something a person is or does). Automated entry control devices based on these techniques are grouped into three categories: coded, credential, and biometric devices.

## **CODED DEVICES**

Coded devices operate on the principle that a person has been issued a code to enter into an entry control device. This code will match the code stored in the device and permit entry. Depending on the application, a single code can be used by all persons authorized to enter the controlled area or each authorized person can be assigned a unique code. Group codes are useful when the group is small and controls are primarily for keeping out the general public. Individual codes are usually required for control of entry to more critical areas. Coded devices verify the entered code's authenticity, and any person entering a correct code is authorized to enter the controlled area. Electronically coded devices include electronic and computer-controlled keypads.

**Electronic Keypad Devices.** The common telephone keypad (12 keys) is an example of an electronic keypad. This type of keypad consists of simple push-button switches that, when depressed, are decoded by digital logic circuits. When the correct sequence of buttons is pushed, an electric signal unlocks the door for a few seconds.

**Computer-controlled Keypad Devices.** These devices are similar to electronic keypad devices, except they are equipped with a microprocessor in the keypad or in a separate enclosure at a different location. The microprocessor monitors the sequence in which the

keys are depressed and may provide additional functions such as personal ID and digit scrambling. When the correct code is entered and all conditions are satisfied, an electric signal unlocks the door.

## CREDENTIAL DEVICES

A credential device identifies a person having legitimate authority to enter a controlled area. A coded credential (e.g., plastic card or key) contains a prerecorded, machine-readable code. An electric signal unlocks the door if the prerecorded code matches the code stored in the system when the card is read. Like coded devices, credential devices only authenticate the credential; it assumes a user with an acceptable credential is authorized to enter. The most commonly used types of cards are described as follows:

**Magnetic-stripe Card.** A strip of magnetic material located along one edge of the card is encoded with data (sometimes encrypted). The data is read by moving the card past a magnetic read head.

**Wiegand-effect Card.** The Wiegand-effect card contains a series of small-diameter, parallel wires approximately ½-inch long, embedded in the bottom half of the card. The wires are manufactured from ferromagnetic materials that produce a sharp change in magnetic flux when exposed to a slowly changing magnetic field. This type of card is impervious to accidental erasure. The card reader contains a small read head and a tiny magnet to supply the applied magnetic field. It usually does not require external power.

**Proximity Card.** A proximity card is not physically inserted into a reader; the coded pattern on the card is sensed when it is brought within several inches of the reader. Several techniques are used to code cards. One technique uses a number of electrically tuned circuits embedded in the card. Data are encoded by varying resonant frequencies of the tuned circuits. The reader contains a transmitter that continually sweeps through a specified range of frequencies and a receiver that senses the pattern of resonant frequencies contained in the card. Another technique uses an



integrated circuit embedded in the card to generate a code that can be magnetically or electro-statically coupled to the reader. The power required to activate embedded circuitry can be provided by a small battery embedded in the card or by magnetically coupling power from the reader.

**Smart Card.** A smart card is embedded with a microprocessor, memory, communication circuitry, and a battery. The card contains edge contacts that enable a reader to communicate with the microprocessor. Entry control information and other data may be stored in the microprocessor's memory.

**Bar Code.** A bar code consists of black bars printed on white paper or tape that can be easily read with an optical scanner. This type of coding is not widely used for entry control applications because it can be easily duplicated. It is possible to conceal the code by applying an opaque mask over it. In this approach, an IR scanner is used to interpret the printed code. For low-level security areas, the use of bar codes can provide a cost-effective solution for entry control. Coded strips and opaque masks can be attached to existing ID badges, alleviating the need for complete badge replacement.

## BIOMETRIC DEVICES

The third basic technique used to control entry is based on the measurement of one or more physical or personal characteristics of an individual. Because most entry control devices based on this technique rely on measurements of biological characteristics, they have become commonly known as biometric devices. Characteristics such as fingerprints, hand geometry, voiceprints, handwriting, and retinal blood-vessel patterns have been used for controlling entry. Typically, in enrolling individuals, several reference measurements are made of the selected characteristic and then stored in the device's memory or on a card. From then on, when that person attempts entry, a scan of the characteristic is compared with the reference data template. If a match is found, entry is granted. Rather than verifying an artifact, such as a code

or a credential, biometric devices verify a person's physical characteristic, thus providing a form of identity verification. Because of this, biometric devices are sometimes referred to as personnel identity verification devices. The most common biometric devices are discussed below.

**Fingerprints.** Fingerprint-verification devices use one of two approaches. One is pattern recognition of the whorls, loops, and tilts of the referenced fingerprint, which is stored in a digitized representation of the image and compared with the fingerprint of the prospective entrant. The second approach is minutiae comparison, which means that the endings and branching points of ridges and valleys of the referenced fingerprint are compared with the fingerprint of the prospective entrant.

**Hand Geometry.** Several devices are available that use hand geometry for personnel verification. These devices use a variety of physical measurements of the hand, such as finger length, finger curvature, hand width, webbing between fingers, and light transmissivity through the skin to verify identity. Both two- and three-dimensional units are available.

**Retinal Patterns.** This type of technique is based on the premise that the pattern of blood vessels on the human eye's retina is unique to an individual. While the eye is focused on a visual target, a low-intensity IR light beam scans a circular area of the retina. The amount of light reflected from the eye is recorded as the beam progresses around the circular path. Reflected light is modulated by the difference in reflectivity between blood-vessel pattern and adjacent tissue. This information is processed and converted to a digital template that is stored as the eye's signature. Users are allowed to wear contact lenses; however, glasses should be removed.

## MONITORING OF DESIGNATED RESTRICTED AREAS

A restricted area is any area that can be monitored by electronic devices and that is subject to special restrictions or controls for security reasons. Restricted areas may be established for the following:

- The enforcement of security measures and the exclusion of unauthorized personnel.
- Intensified controls in areas requiring special protection.
- The protection of classified information or critical equipment or materials.

## DEGREE OF SECURITY

The degree of security and control required depends on the nature, sensitivity, or importance of the security interest. Restricted areas are classified as controlled, limited, or exclusion areas:

**Controlled Area.** A controlled area is that portion of a restricted area usually near or surrounding a limited or exclusion area. Entry to the controlled area is restricted to personnel with a need for access. Movement of authorized personnel within this area is not necessarily controlled because mere entry to the area does not provide access to the security interest. The controlled area is provided for administrative control, for safety, or as a buffer zone for indepth security for the limited or exclusion area.

**Limited Area .** A limited area is a restricted area within close proximity of a security interest. Uncontrolled movement may permit access to the item. Escorts and other internal restrictions may prevent access within limited areas.

**Exclusion Area.** An exclusion area is a restricted area containing a security interest. Uncontrolled movement permits direct access to the item.

There are other important considerations concerning restricted areas and their lines of division. These considerations include the following:

- A survey and analysis of the facility, its missions, and its security interests. This can determine immediate and anticipated needs that require protection. Anticipated needs are determined from plans for the future.
- The size and nature of the security interest being protected. Safes may provide adequate protection for classified documents and small items; however, large items may have to be placed within guarded enclosures.
- Some security interests are more sensitive to compromise than others. Brief observation or a simple act by an untrained person may constitute a compromise in some cases. In others, detailed study and planned action by an expert may be required.

**American Association of State Highway and Transportation Officials**

*A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection*, May 2002 , The American Association of State Highway and Transportation Officials' Security Task Force, Washington, DC  
<http://security.transportation.org/community/security/guides.html>

**The American Institute of Architects**

*Building Security Through Design: A Primer for Architects, Design Professionals, and their Clients*, November 2001, The American Institute of Architects (book)  
<http://www.aia.org/security>

**American Institute of Chemical Engineers**

Pub No: G-79, *Guidelines for Analyzing and Managing the Security Vulnerabilities at Fixed Chemical Sites*, 2002, Center for Chemical Process Safety, ISBN No: 0-8169-0877-X  
<http://www.aiche.org/ccpssecurity>

**American Medical Association**

*Physical injuries and fatalities resulting from the Oklahoma City bombing*, August 7, 1996, S. Mallonee, S. Shariat, G. Stennies, R. Waxweiler, D. Hogan, and F. Jordan., The Journal of the American Medical Association, Vol. 276 No. 5., pp 382-387  
Abstract at URL:  
<http://jama.ama-assn.org/cgi/content/abstract/276/5/382>

**American Society of Civil Engineers**

Architectural Engineering Institute of American Society of Civil Engineers, AEI Newsletter, *The Team, Special Terrorism Issue*, Fall 2001, Volume 4, Issue 3  
[http://www.asce.org/pdf/aei\\_11\\_1.pdf](http://www.asce.org/pdf/aei_11_1.pdf)

*Blast Effects on Buildings: Design of Buildings to Optimize Resistance to Blast Loading*, 1995, G.C. Mays and P.D. Smith, London: Thomas Telford, Ltd., American Society of Civil Engineers, ISBN: 0-7277-2030-9  
<http://www.pubs.asce.org/BOOKdisplay.cgi?9990338>

*Blast Resistant Design of Commercial Buildings*, 1996, M. Ettouney, R. Smilowitz, and T. Rittenhouse, Practice Periodical on Structural Design and Construction, Vol. 1, No. 1, February 1996, American Society of Civil Engineers  
<http://ojps.aip.org/dbt/dbt.jsp?KEY=PPSCFX&Volume=1&Issue=1>  
A preprint of the final article is available at  
<http://www.wai.com/AppliedScience/Blast/blast-struct-design.html>

*Design of Blast Resistant Buildings in Petrochemical Facilities*, 1997, American Society of Civil Engineers, ISBN: 0-7844-0265-5  
<http://www.pubs.asce.org/BOOKdisplay.cgi?9704510>

*Glass-Related Injuries in Oklahoma City Bombing*, Journal of Performance of Constructed Facilities, May 1999, 13, No. 2, H Scott Norville, Natalie Harville, Edward J. Conrath, Sheryll Shariat, and Sue Mallonee  
<http://www.pubs.asce.org/WWWdisplay.cgi?9902006>

*Lessons from the Oklahoma City Bombing: Defensive Design Techniques*, January 1997, Eve E. Hinman and David J. Hammond, January 1997, American Society of Civil Engineers (ASCE Press), Reston, VA, ISBN: 0784402175  
<http://www.asce.org/publications/booksdisplay.cfm?type=9702295>

*Minimum Design Loads for Buildings and Other Structures*, ASCE 7-02, 2002, American Society of Civil Engineers, ISBN: 0-7844-0624-3 [Note revision of 7-98, does not include building security or antiterrorism, but covers all natural hazards]  
<http://www.pubs.asce.org/ASCE7.html?9991330>

Structural Engineering Institute of American Society of Civil Engineers, *Structural Design for Physical Security: State of the Practice*, 1999, Edward Conrath, et al., Reston, VA, Structural Engineering Institute of American Society of Civil Engineers  
<http://www.pubs.asce.org/BOOKdisplay.cgi?9990571>

*Vulnerability and Protection of Infrastructure Systems: The State of the Art*,  
An ASCE Journals Special Publication compiling articles from 2002  
and earlier available online

[https://ascestore.aip.org/OA\\_HTML/aipCCtpItmDspRte.jsp?a=b  
& item=39885](https://ascestore.aip.org/OA_HTML/aipCCtpItmDspRte.jsp?a=b&item=39885)

### **American Society of Heating, Refrigerating, and Air-Conditioning Engineers**

*Defensive Filtration*, ASHRAE Journal, December 2002, James D. Miller  
[http://resourcecenter.ashrae.org/store/ashrae/  
newstore.cgi?itemid= 9346&view=item&categoryid=409&page=1&l  
oginid=29483](http://resourcecenter.ashrae.org/store/ashrae/newstore.cgi?itemid=9346&view=item&categoryid=409&page=1&loginid=29483)

*Report of Presidential Ad Hoc Committee for Building Health and Safety  
under Extraordinary Incidents on Risk Management Guidance for Health,  
Safety and Environmental Security under Extraordinary Incidents*,  
Washington, DC, January 26, 2003  
<http://xp20.ashrae.org/about/extraordinary.pdf>

*Risk Management Guidance for Health and Safety under Extraordinary  
Incidents*, ASHRAE 2002 Winter Meeting Report, January 12, 2002  
<http://atfp.nfesc.navy.mil/pdf/ASHRAE%20CBR%20Guidance.pdf>  
or  
[http://engineering.tamu.edu/safety/guidelines/faclab/ASHRAE\\_  
Security\\_Rpt\\_12Jan02.pdf](http://engineering.tamu.edu/safety/guidelines/faclab/ASHRAE_Security_Rpt_12Jan02.pdf)

Standard 62-2001, *Ventilation for Acceptable Indoor Air Quality* (ANSI  
Approved), ISSN 1041-2336, addenda to basic ANSI/ASHRAE  
Standard 62 basic (1989)  
[http://resourcecenter.ashrae.org/store/ashrae/newstore.cgi?  
itemid= 6852&view=item&categoryid=311&page=1&loginid=29483](http://resourcecenter.ashrae.org/store/ashrae/newstore.cgi?itemid=6852&view=item&categoryid=311&page=1&loginid=29483)

### **Building Owners and Managers Association International**

*How to Design and Manage Your Preventive Maintenance Program*, 1996  
<http://www.boma.org/pubs/bomampm.htm>

## **Centers for Disease Control and Prevention/ National Institute for Occupational Safety and Health**

Publication No. 2002-139, *Guidance for Protecting Building  
Environments from Airborne Chemical, Biological, or Radiological Attacks*,  
May 2002, Cincinnati, OH  
<http://www.cdc.gov/niosh/bldvent/2002-139.html>

Publication No. 2003-136, *Guidance for Filtration and Air Cleaning  
Systems to Protect Building Environments from Airborne Chemical,  
Biological, or Radiological Attacks*, April 2003, Cincinnati, OH  
<http://www.cdc.gov/niosh/docs/2003-136/2003-136.html>

## **Central Intelligence Agency**

*Chemical, Biological, Radiological Incident Handbook*, October 1998  
[http://www.cia.gov/cia/publications/cbr\\_handbook/cbrbook.htm](http://www.cia.gov/cia/publications/cbr_handbook/cbrbook.htm)

## **Council on Tall Buildings and Urban Habitat**

*Building Safety Enhancement Guidebook*, 2002  
<http://www.ctbuh.org>

*Task Force on Tall Buildings: "The Future,"* October 15, 2001  
[http://www.lehigh.edu/ctbuh/htmlfiles/hot\\_links/report.pdf](http://www.lehigh.edu/ctbuh/htmlfiles/hot_links/report.pdf)  
or [http://www.ctbuh.org/htmlfiles/hot\\_links/report.pdf](http://www.ctbuh.org/htmlfiles/hot_links/report.pdf)

## **Federal Aviation Administration**

DOT/FAA/AR-00/52, *Recommended Security Guidelines for Airport  
Planning, Design and Construction*, Revised June 2001, Associate  
Administrator for Civil Aviation Security Office of Civil Aviation  
Security, Policy and Planning, Federal Aviation Administration,  
Washington, DC 20591 (not available on Internet)

FAA Order 1600.69A, *FAA Facility Security Management Program*,  
updated FAA Order 1600.69B to be published shortly – The  
Federal Aviation Administration's criteria for the protection of its  
facilities. *[For Official Use Only]* (not available on Internet)



## **Federal Emergency Management Agency**

FEMA 152, *Seismic Considerations: Apartment Buildings, Earthquake Hazards Reduction Series 37*, November 1988, Washington, DC (not available on Internet) Contact FEMA Distribution Center, P.O. Box 2012, 8231 Stayton Drive, Jessup, MD 20794-2012, Telephone: 1-800-480- 2520, Fax: 301-362-5335

FEMA 153, *Seismic Considerations: Office Buildings, Earthquake Hazards Reduction Series 38*, November 1988, Washington, DC (not available on Internet) Contact FEMA Distribution Center, P.O. Box 2012, 8231 Stayton Drive, Jessup, MD 20794-2012, Telephone: 1-800-480-2520, Fax: 301-362-5335

FEMA 154, *Rapid Visual Screening of Buildings for Seismic Hazards: A Handbook (2<sup>nd</sup> Edition)*, 2002, 1988, Washington, DC (not available on Internet) Contact FEMA Distribution Center, P.O. Box 2012, 8231 Stayton Drive, Jessup, MD 20794-2012, Telephone: 1-800-480-2520, Fax: 301-362-5335

FEMA 277, *The Oklahoma City Bombing: Improving Building Performance through Multi-Hazard Mitigation*, August 1, 1996, Washington, DC  
<http://www.fema.gov/mit/bpat/bpat009.htm>

FEMA 372, *Mitigation Resources for Success (CD-ROM)*, October 2001, Washington, DC  
[http://www.fema.gov/pdf/library/poster\\_fnl2.pdf](http://www.fema.gov/pdf/library/poster_fnl2.pdf)

FEMA 386-2, *Understanding Your Risks, Identifying Hazards and Estimating Losses*, August 2001  
[http://www.fema.gov/fima/planning\\_toc3.shtm](http://www.fema.gov/fima/planning_toc3.shtm)

FEMA 386-7, *Integrating Human-Caused Hazards Into Mitigation Planning*, September 2002  
<http://www.fema.gov/fima/antiterrorism/resources.shtm>

FEMA 403, *World Trade Center Building Performance Study: Data Collection, Preliminary Observations, and Recommendations*, May 2002, Washington, DC  
<http://www.fema.gov/library/wtcstudy.shtm>

State and Local Guide 101, *Guide for All-Hazard Emergency Operations Planning, Chapter 6, Attachment G, Terrorism*, April 2001  
<http://www.fema.gov/rrr/allhzpln.shtm>

### **General Services Administration**

*Balancing Security and Openness: A Thematic Summary of a Symposium on Security and the Design of Public Buildings*, November 30, 1999  
[http://hydra.gsa.gov/pbs/pc/gd\\_files/SecurityOpenness.pdf](http://hydra.gsa.gov/pbs/pc/gd_files/SecurityOpenness.pdf)

*Cost Impact of ISC Security Criteria*, GSA & Applied Research Associates, Inc., L. Bryant and J. Smith, Vicksburg, MS  
**[Restricted Access]**  
<http://www.oca.gsa.gov/specialphp/References.php>

*Facility Standards for the Public Building Service (PBS-P100)*; Chapter 8, Security Design, Revised November 2000  
<http://hydra.gsa.gov/pbs/pc/facilitiesstandards/>

*Mail Center Manager's Security Guide – Second Edition*, October 22, 2002  
[http://www.gsa.gov/attachments/GSA\\_PUBLICATIONS/extpub/MailCenterManagersSecurityGuideV2.pdf](http://www.gsa.gov/attachments/GSA_PUBLICATIONS/extpub/MailCenterManagersSecurityGuideV2.pdf)

Progressive Collapse Analysis and Design Guidelines for New Federal Office Buildings and Major Modernization Projects, November 2000 **[Restricted Access]**  
<http://www.oca.gsa.gov/specialphp/References.php>

*Security Reference Manual*, Part 3: Blast Design and Assessment Guidelines, July 31, 2001 **[For Official Use Only]** **[Restricted Access]**  
<http://www.oca.gsa.gov/specialphp/References.php>

### **Healthy Building International, Inc.**

*Vulnerability Assessments and Counter Terrorist Protocols*  
<http://www.healthybuildings.com/s2/vacbt.pdf>

### **Interagency Security Committee (executive agent – GSA)**

*ISC Security Design Criteria for New Federal Office Buildings and Major Modernization Projects*, May 28, 2001, **[For Official Use Only]**

*[Restricted Access]*

<http://www.oca.gsa.gov/specialphp/References.php>

### **Institute of Transportation Engineers**

*The Influence of Traffic Calming Devices upon Fire Vehicle Travel Times*,  
Michael A. Coleman, 1997, ITE Annual Meeting Compendium,  
1997 pp. 838-845

<http://webservices.camsys.com/fhwa/cmn/cmn33.htm>

*Split Speed Bump*, 1998, Kathy Mulder, Washington, DC, TE  
International Conference, 1998

<http://www.ite.org/traffic/documents/CCA98A33.pdf>

### **Lawrence Berkeley National Lab**

*Protecting Buildings From a Biological or Chemical Attack: actions to take  
before or during a release*. LBNL/PUB-51959, January 10, 2003

<http://securebuildings.lbl.gov/images/bldgadvice.pdf>

### **National Academy of Sciences**

*Combating Terrorism: Prioritizing Vulnerabilities and Developing  
Mitigation Strategies*, Project Identification Number: NAEP-R-02-01-  
A, National Academy of Engineering on-going project – results to  
be published.

[http://www4.nationalacademies.org/webcr.nsf/ProjectScopeDisplay/  
NAEP-R-02-01-A?OpenDocument](http://www4.nationalacademies.org/webcr.nsf/ProjectScopeDisplay/NAEP-R-02-01-A?OpenDocument)

### **National Capital Planning Commission**

*Designing for Security in the Nation's Capital*, October 2001

[http://www.ncpc.gov/planning\\_init/security/DesigningSec.pdf](http://www.ncpc.gov/planning_init/security/DesigningSec.pdf)

*The National Capital Planning Urban Design and Security Plan*,  
October 2002

<http://www.ncpc.gov/publications/udsp/Final%20UDSP.pdf>

### **National Institute of Building Sciences**

*Whole Building Design Guide: Provide Security for Building Occupants and Assets*

<http://www.wbdg.org/design/index.php?cn=2.7.4&cx=0>

### **National Research Council**

*Protecting Buildings and People from Terrorism: Technology Transfer for Blast-effects Mitigation*, 2001, National Academy Press, Washington, DC, ISBN 0-309-08286-2

<http://books.nap.edu/books/0309082862/html/index.html>

*Protecting Buildings From Bomb Blast, Transfer of Blast-Effects Mitigation Technologies from Military to Civilian Applications*, 1995, National Academy Press, Washington, DC, ISBN 0-309-05375-7

<http://books.nap.edu/books/0309053757/html/index.html>

*Protection of Federal Office Buildings Against Terrorism*, 1988, Committee on the *Protection of Federal Facilities Against Terrorism*, Building Research Board, National Academy Press, Washington, DC, ISBN 0-309-07691-9

<http://books.nap.edu/books/0309076463/html/index.html>

### **Society of American Military Engineers**

National Symposium of Comprehensive Force Protection, October 2001, Charleston, SC, Lindbergh & Associates. For a list of participants, access

<http://www.same.org/forceprot/force.htm>

### **Technical Support Working Group (TSWG)**

*Terrorist Bomb Threat Stand-Off Card with Explanation of Use*

[http://www.tswg.gov/tswg/prods\\_pubs/newBTSCPress.htm](http://www.tswg.gov/tswg/prods_pubs/newBTSCPress.htm)

### **The House National Security Committee**

Statement of Chairman Floyd D. Spence on the Report of the Bombing of Khobar Towers, August 1996, Washington, DC

<http://www.house.gov/hasc/Publications/104thCongress/Reports/saudi.pdf>

## **U.S. Air Force**

ESL-TR-87-57, *Protective Construction Design Manual*, November 1989; Contact Airbase Technologies Division (AFRL/MLQ) at Tyndall Air Force Base, FL, via e-mail to [techinfo@afrl.af.mil](mailto:techinfo@afrl.af.mil). [Superseded by Army Technical Manual TM 5-855-1 (Air Force Pamphlet AFPAM 32-1147(I), Navy Manual NAVFAC P-1080, DSWA Manual DAHSCWEMAN-97), December 1997]

*Expedient Hardening Methods for Structures Subjected to the Effect of Nonnuclear Munitions*, October 1990, Wright Laboratory Report (not available on Internet)

*Installation Entry Control Facilities Design Guide*, October 2002, Air Force Center for Environmental Excellence

<http://www.afcee.brooks.af.mil/dc/dcd/gate/index.html>

*Installation Force Protection Guide*, 1997, Air Force Center for Environmental Excellence

<http://www.afcee.brooks.af.mil/dc/dcd/arch/force.pdf>

*Vehicle Bomb Mitigation Guide*, July 1, 1999, Force Protection Battlelab [**For Official Use Only**] Contact the USAF Force Protection Battlelab, Lackland Air Force Base, TX, Telephone: (210)671-0058

## **U.S. Army**

### **Field Manuals (FM)**

FM 3-19.30, *Physical Security*, January 8, 2001, Washington, DC  
<http://www.adtdl.army.mil/cgi-bin/atdl.dll/fm/3-19.30/fm3-19.30.pdf>  
or

[http://www.wood.army.mil/mpdoctrine/PDF\\_Files/FM\\_3-19.30.pdf](http://www.wood.army.mil/mpdoctrine/PDF_Files/FM_3-19.30.pdf)

FM 5-114, *Engineer Operations Short of War*, July 13, 1992  
<http://155.217.58.58/cgi-bin/atdl.dll/fm/5-114/toc.htm>

Technical Instruction 853-01 (Draft), *Protecting Buildings and Their Occupants from Airborne Hazards*, October 2001  
[http://buildingprotection.sbccom.army.mil/basic/airborne\\_hazards](http://buildingprotection.sbccom.army.mil/basic/airborne_hazards)

## **U.S. Army Corps of Engineers**

### **Engineer Technical Letters (ETL)**

ETL 1110-3-494, *Airblast Protection Retrofit for Unreinforced Concrete Masonry Walls*, July 14, 1999 [**Restricted Access**]  
<http://www.usace.army.mil/inet/usace-docs/eng-tech-ltrs>

ETL 1110-3-495, *Estimating Damage to Structures from Terrorist Bombs Field Operations Guide*, July 14, 1999 [**Restricted Access**]  
<http://www.usace.army.mil/inet/usace-docs/eng-tech-ltrs>

ETL 1110-3-498, *Design of Collective Protection Shelters to Resist Chemical, Biological, and Radiological (CBR) Agents*, February 24, 1999  
<http://www.usace.army.mil/inet/usace-docs/eng-tech-ltrs>

ETL 1110-3-501, *Window Retrofit Using Fragment Retention Film with Catcher Bar System*, July 14, 1999 [**Restricted Access**]  
<http://www.usace.army.mil/inet/usace-docs/eng-tech-ltrs>

### **Protective Design – Mandatory Center of Expertise – Technical Reports**

PDC-TR-91-6, *Blast Analysis Manual, Part 1 – Level of Protection Assessment Guide*, July 1991 [**For Official Use Only**]  
Contact U.S. Army Corps of Engineers Protective Design Center, ATTN: CENWO-ED-ST, 215 N. 17th Street, Omaha, NE 68102-4978, Telephone: (402)221-4918

### **Technical Manuals (TM)**

TM 5-853-1, *Security Engineering Project Development*, May 12, 1994, also Air Force Manual 32-1071, Volume 1  
[**For Official Use Only**]  
<http://www.usace.army.mil/inet/usace-docs/armytm>

TM 5-853-2, *Security Engineering Concept Design*, May 12, 1994, also Air Force Manual 32-1071, Volume 2  
[**For Official Use Only**]  
<http://www.usace.army.mil/inet/usace-docs/armytm>

TM 5-853-3, *Security Engineering Final Design*, May 12, 1994, also Air Force Manual 32-1071, Volume 3

**[For Official Use Only]**

<http://www.usace.army.mil/inet/usace-docs/armytm>

TM 5-853-4, *Security Engineering Electronic Security Systems*,  
May 12, 1994

<http://www.usace.army.mil/inet/usace-docs/armytm>

TM 5-855-4, *Heating, Ventilation, and Air Conditioning of  
Hardened Installations*, November 28, 1986

<http://www.usace.army.mil/inet/usace-docs/armytm/tm5-855-4/toc.htm>

TM 5-1300, *Structures to Resist Accidental Explosions*,  
November 19, 1990, (also Navy NAVFAC (Naval Facilities)  
P-397, Air Force Regulation 88-2); Contact David Hyde,  
U.S. Army Engineer Research and Development Center,  
3909 Halls Ferry Road, Vicksburg, MS 39180 or via e-mail  
to [hyded@ex1.wes.army.mil](mailto:hyded@ex1.wes.army.mil)

## **U.S. Department of Commerce**

### **Administrative Orders (DAO)**

DAO 206-5, *Occasional Use of Public Areas in Public Buildings*,  
December 9, 1986

<http://www.osec.doc.gov/bmi/daos/206-5.htm>

DAO 207-1, *Security Programs*, June 24, 1991, Amended  
September 6, 1991

<http://www.osec.doc.gov/bmi/daos/207-1.htm>

### **Critical Infrastructure Assurance Office**

*Vulnerability Assessment Framework 1.1*, October 1998

<http://www.ciao.gov/resource/vullassessframework.pdf>

*Practices For Securing Critical Information Assets*, January 2000

[http://www.ciao.gov/resource/Practices\\_For\\_Securing\\_Critical\\_Information\\_Assets.pdf](http://www.ciao.gov/resource/Practices_For_Securing_Critical_Information_Assets.pdf)

## **U.S. Department of Defense**

*DoD Security Engineering Manual* [Expected to have a major portion for public distribution once published as Unified Facilities Criteria and a smaller portion For Official Use Only similar to the UFC for AT Standards for Buildings listed below. This publication will replace Army Technical Manual 5-853 (Air Force Joint Manual 32-1071), Volumes 1, 2, and 3 and Navy Military Handbook 1013/1A]

DoD O-2000.12-H, *Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence: Mandatory Standards and Implementing Guidance, with Changes 1 and 2*, February 1993, Change 1 — May 21, 1993, Change 2 – October 3, 1997

**[For Official Use Only]**

<http://www.dtic.mil/whs/directives/corres/pub1.html>

Force Protection Equipment Demonstration IV, 6-8 May 2003

<http://www.fped4.org>

*Interim Antiterrorism/Force Protection Construction Standards*, December 16, 1999 **[For Official Use Only]** Contact U.S. Army Engineer District, Omaha, NE ATTN: CENWO-ED-ST, 215 North 17<sup>th</sup> Street, Omaha, NE 68102-4978, Telephone: (402)221-4918.

*Interim Antiterrorism/Force Protection Construction Standards—Progressive Collapse Guidance*, April 4, 2000 (not available on Internet) Contact U.S. Army Corps of Engineers Protective Design Center, ATTN: CENWO-ED-ST, 215 N. 17th Street, Omaha, NE 68102-4978, Telephone: (402)221-4918

### **Unified Facilities Criteria (UFC)**

UFC 3-340-01, *Design and Analysis of Hardened Structures to Conventional Weapons Effects*, June 30, 2002

**[For Official Use Only]** [Formerly Army TM 5-855-1]

<http://www.hnd.usace.army.mil/techinfo/ufc/UFC3-340-01.WEB.PDF>

UFC 4-010-01, *DoD Minimum Antiterrorism Standards for Buildings*, July 31, 2002

<http://www.wbdg.org/ccbref/ccbdoc.php?category=ufc&docid=106&ref=1>



## Unified Facilities Guide Specifications (UFGS)

UFGS-02821A, *Fencing*, February 2002

<http://www.ccb.org/ufigs/pdf/02821A.pdf>

UFGS-02840A, *Active Vehicle Barriers*, February 2002

<http://www.ccb.org/ufigs/pdf/02840A.pdf>

UFGS-02841N, *Traffic Barriers*, August 2001

<http://www.ccb.org/ufigs/pdf/02841N.pdf>

UFGS-08390A, *Blast Resistant Doors*, April 2001

<http://www.ccb.org/ufigs/pdf/08390.pdf>

UFGS-08581, *Blast Resistant Tempered Glass Windows*,  
August 2001

<http://www.ccb.org/ufigs/pdf/08581.pdf>

UFGS-08840A, *Plastic Glazing*, July 1995

<https://www.ccb.org/ufigs/pdf/08840A.pdf>

UFGS-08850, *Fragment Retention Film for Glass*, July 1992

<https://www.ccb.org/ufigs/pdf/08850.pdf>

UFGS-11020, *Security Vault Door*, August 2002

<http://www.ccb.org/ufigs/pdf/11020.pdf>

UFGS-11025, *Forced Entry Resistant Components*, August 2001

<http://www.ccb.org/ufigs/pdf/11025.pdf>

UFGS-11035, *Bullet-Resistant Components*, April 2000

<http://www.ccb.org/ufigs/pdf/11035.pdf>

UFGS-13095A, *Electromagnetic (EM) Shielding*, July 2001

<http://www.ccb.org/ufigs/pdf/13095A.pdf>

UFGS-13420A, *Self-Acting Blast Valves*, November 1997

<http://www.ccb.org/ufigs/pdf/13420A.pdf>

## U.S. Department of Energy

DOE/TIC 11268, *A Manual for the Prediction of Blast and Fragment Loadings on Structures*, February 1992, Albuquerque, NM, Southwest Research Institute [not available on Internet]

## **U.S. Department of Homeland Security**

*National Strategy for Homeland Security*, July 2002

[http://www.dhs.gov/interweb/assetlibrary/nat\\_strat\\_hls.pdf](http://www.dhs.gov/interweb/assetlibrary/nat_strat_hls.pdf)

*The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, February 2003

[http://www.dhs.gov/interweb/assetlibrary/Physical\\_Strategy.pdf](http://www.dhs.gov/interweb/assetlibrary/Physical_Strategy.pdf)

National Strategy to Secure Cyberspace, February 2003

[http://www.dhs.gov/interweb/assetlibrary/National\\_Cyberspace\\_Strategy.pdf](http://www.dhs.gov/interweb/assetlibrary/National_Cyberspace_Strategy.pdf)

*President's Homeland Security Advisory Council - Statewide Template Initiative*, March 2003

[http://www.dhs.gov/interweb/assetlibrary/Statewide\\_Template\\_Initiative.pdf](http://www.dhs.gov/interweb/assetlibrary/Statewide_Template_Initiative.pdf)

*State and Local Actions for Homeland Security*, July 2002

[http://www.whitehouse.gov/homeland/stateandlocal/State\\_and\\_Local\\_Actions\\_for\\_Homeland\\_Security.pdf](http://www.whitehouse.gov/homeland/stateandlocal/State_and_Local_Actions_for_Homeland_Security.pdf)

## **U.S. Department of Housing and Urban Development**

*The Avoidance of Progressive Collapse, Regulatory approaches to the problem*, PB-248 781, October 1975, Division of Energy, Building Technology and Standards, Office of Policy Development and Research, Washington, DC 20410 (not available on Internet)

*Creating Defensible Space*, April 1996, Oscar Newman, Washington, DC

<http://www.huduser.org>

## **U.S. Department of Justice**

### **Federal Bureau of Investigation (FBI)**

*Terrorism in the United States, 1999*, Washington, DC,  
Counterterrorism Division

<http://www.fbi.gov/publications.htm>

## Office of Domestic Preparedness (ODP)

*Fiscal Year 1999 State Domestic Preparedness Equipment Program, Assessment and Strategy Development Tool Kit*, NCJ181200, May 15, 2000, [**For Official Use Only**]  
<http://www.ojp.usdoj.gov/odp/docs/assessment.txt>

## National Institute of Justice (NIJ)

*The Appropriate and Effective Use of Security Technologies in U.S. Schools: A Guide for Schools and Law Enforcement Agencies*, September 1999, with U.S. Department of Education, Safe and Drug-Free Schools Program; and U.S. Department of Energy, Sandia National Laboratories  
<http://www.ncjrs.org/school/home.html>

NIJ Guide 100-00, *Guide for the Selection of Chemical Agent and Toxic Industrial Material Detection Equipment for Emergency First Responders*, June 2000  
<http://www.ncjrs.org/pdffiles1/nij/184449.pdf>

NIJ Guide 101-00, *An Introduction to Biological Agent Detection Equipment for Emergency First Responders*, December 2001  
<http://www.ncjrs.org/pdffiles1/nij/190747.pdf>

NIJ Guide 102-00, *Guide for the Selection of Personal Protective Equipment for Emergency First Responders*, Volumes I-IV, November 2002  
<http://www.ncjrs.org/pdffiles1/nij/191518.pdf>

NIJ Guide 602-00, *Guide to the Technologies of Concealed Weapon and Contraband Imaging and Detection*, February 2001  
<http://www.ncjrs.org/pdffiles1/nij/184432.pdf>

NIJ Standard 0108.01, *Blast Resistant Protective Materials*, September 1985 [**Subscription Required**]  
<http://www.ccb.org>

*Crime Prevention Through Environmental Design and Community Policing*, August 1996, Dan Fleissner and Fred Heinzelmann, Washington, DC

<http://www.ncjrs.org/pdffiles/crimepre.pdf>

*Crime Prevention Through Environmental Design in Parking Facilities*, April 1996, Mary S. Smith, Washington, DC

<http://www.ncjrs.org/pdffiles/cptedpkg.pdf>

*“Designing Out” Gang Homicides and Street Assaults*, November 1998, James Lasley, Washington, DC

<http://www.ncjrs.org/pdffiles/173398.pdf>

*The Expanding Role of Crime Prevention Through Environmental Design in Premises Liability*, April 1996, Corey L. Gordon and William Brill Washington, DC

<http://www.ncjrs.org/pdffiles/cptedlia.pdf>

*Physical Environment and Crime*, January 1996, Ralph B. Taylor and Adele V. Harrell, Washington, DC

<http://www.ncjrs.org/pdffiles/physenv.pdf>

*Visibility and Vigilance: Metro’s Situational Approach to Preventing Subway Crime*, November 1997, Nancy G La Vigne, Washington, DC

<http://www.ncjrs.org/pdffiles/166372.pdf>

#### **U.S. Marshals Service**

*Vulnerability Assessment of Federal Facilities*, June 28, 1995

[Restricted Access]

<http://www.oca.gsa.gov>

#### **U.S. Department of State, Bureau of Diplomatic Security**

*Architectural Engineering Design Guidelines* (5 Volumes), March 1998  
[For Official Use Only] (not available on Internet)

Certification Standard SD-STD-01.01, Revision G (Amended),  
*Forced Entry and Ballistic Resistance of Structural Systems*, Amended

April 30, 1993 [**Subscription Required**]

<http://www.ccb.org>

*Patterns of Global Terrorism, 2002*, April 2002, Washington, DC

<http://www.state.gov/s/ct/rls/pgtrpt/2002/pdf/>

*Physical Security Standards Handbook*, January 7, 1998 [**For Official Use Only**] (not available on Internet)

*Structural Engineering Guidelines for New Embassy Office Buildings*, August 1995 [**For Official Use Only**] (not available on Internet)

*The Report of the Accountability Review Board on the Embassy Bombings in Nairobi and Dar es Salaam on August 7, 1998*, January 1999, Washington, DC

[http://www.state.gov/www/regions/africa/accountability\\_report.html](http://www.state.gov/www/regions/africa/accountability_report.html)

### **U.S. Department of the Treasury/Bureau of Alcohol, Tobacco, and Firearms**

*Vehicle Bomb Explosion Hazard And Evacuation Distance Tables*, 1999, request in writing, address information available at

[http://www.atf.treas.gov/pub/fire-explo\\_pub/i54001.htm](http://www.atf.treas.gov/pub/fire-explo_pub/i54001.htm)

### **U.S. Department of Veterans Affairs**

*Physical Security Assessment of Veterans Affairs Facilities*,

Recommendations of the National Institute of Building Sciences Task Group to the Department of Veterans Affairs, 6 September 2002

<http://www.va.gov/facmgt/standard/etc/vaphysicalsecurityreport.pdf>

### **U.S. Fire Administration (USFA of FEMA)**

*The Critical Infrastructure Protection Process Job Aid*, May 1, 2002

<http://www.usfa.fema.gov/dhtml/fire-service/cipc-jobaid.cfm>

### **U.S. Navy**

**Design Manuals (DM) NAVFAC (Naval Facilities Command)**

NAVFAC DM 2.08, *Blast Resistant Structures*, December 1986

<http://www.wbdg.org/ccbref/ccbdoc.php?category=nav&dodid=46&ref=1>

NAVFAC DM 13.02, *Commercial Intrusion Detection Systems (IDS)*, September 1986  
<http://www.wbdg.org/ccbref/ccbdoc.php?category=nav&docid=47&ref=1>

**Interim Technical Guidance (ITG) 03-03, *Entry Control Facilities***, 20 February 2003  
[http://www.lantdiv.navfac.navy.mil/servlet/page?pageid=8609,8611&\\_dad=lantdiv&\\_schema=LANTDIV&11435\\_ACTIVE\\_1777132.p\\_subid=60007&11435\\_ACTIVE\\_1777132.p\\_sub\\_siteid=51&11435\\_ACTIVE\\_1777132.p\\_edit=0](http://www.lantdiv.navfac.navy.mil/servlet/page?pageid=8609,8611&_dad=lantdiv&_schema=LANTDIV&11435_ACTIVE_1777132.p_subid=60007&11435_ACTIVE_1777132.p_sub_siteid=51&11435_ACTIVE_1777132.p_edit=0)

### **Military Handbooks (MIL-HDBK)**

MIL-HDBK-1002/1, *Structural Engineering General Requirements*, November 30, 1987  
<http://www.wbdg.org/ccbref/ccbdoc.php?category=nav&docid=48&ref=1>

MIL-HDBK-1004/4, *Electrical Utilization Systems*, October 13, 1987  
<http://www.wbdg.org/ccbref/ccbdoc.php?category=nav&docid=49&ref=1>

MIL-HDBK-1012/3, *Telecommunications Premises Distribution Planning, Design, and Estimating*, May 31, 1996  
<http://www.wbdg.org/ccbref/ccbdoc.php?category=nav&docid=50&ref=1>

MIL-HDBK-1013/1A, *Design Guidelines for Physical Security of Fixed Land-Based Facilities*, December 15, 1993. For copies, contact Defense Printing Service, Building 40, 700 Robbins Avenue, Philadelphia, PA 19111-5094, Telephone: (215)697-2179, Fax: (215)697-1462 or available on the National Institute of Building Sciences' Construction Criteria Base

MIL-HDBK-1013/10, *Design Guidelines for Security Fencing, Gates, Barriers, and Guard Facilities*, May 14, 1993. For copies, contact Defense Printing Service, Building 40, 700

Robbins Avenue, Philadelphia, PA 19111-5094, Telephone: (215)697-2179, Fax: (215) 697-1462 or available on the National Institute of Building Sciences' Construction Criteria Base

MIL-HDBK-1013/12, *Evaluation of Security Glazing for Ballistic, Bomb, and Forced Entry Tactics*, March 10, 1997. For copies, contact Defense Printing Service, Building 40, 700 Robbins Avenue, Philadelphia, PA 19111-5094, Telephone: (215)697-2179, Fax: (215) 697-1462 or available on the National Institute of Building Sciences' Construction Criteria Base

MIL-HDBK-1013/14, *Selection and Application of Vehicle Barriers*, February 1, 1999. For copies, contact Defense Printing Service, Building 40, 700 Robbins Avenue, Philadelphia, PA 19111-5094, Telephone: (215)697-2179, Fax: (215)697-1462 or available on the National Institute of Building Sciences' Construction Criteria Base

**TechData Sheets – Naval Facilities Engineering Service Center (NFESC)**

TDS-2062-SHR, *Estimating Damage to Structures from Terrorist Bombs*, September 1998 [**For Official Use Only**] Requests for publication can be made to Naval Facilities Engineering Service Center, Security Engineering Division (ESC66), 1100 23rd Ave, Port Hueneme, CA 93043-4370, Telephone (805)982-1582 (Primary), (805)982-4817 (Alternate); Fax: (805)982-1253

TDS-2063-SHR, *Blast Shielding Walls*, September 1998 [**For Official Use Only**] Requests for publication can be made to Naval Facilities Engineering Service Center, Security Engineering Division (ESC66), 1100 23rd Ave., Port Hueneme, CA 93043-4370, Telephone: (805)982-1582 (Primary), (805)982-4817 (Alternate); Fax: (805)982-1253

TDS-2079-SHR, *Planning and Design Considerations for Incorporating Blast Mitigation in Mailrooms*, May 2000. For copies, contact Defense Printing Service, Building 40, 700

Robbins Avenue, Philadelphia, PA 19111-5094, Telephone:  
(215)697-2179, Fax: (215) 697-1462

TDS-2090-SHR, *Design Parameters for a Controlled Entry Point*.  
For copies, contact Defense Printing Service, Building  
40, 700 Robbins Avenue, Philadelphia, PA 19111-5094,  
Telephone: (215)697-2179, Fax: (215)697-1462

#### **User Guides — Naval Facilities Engineering Service Center (NFESC)**

UG-2030-SHR, *Security Glazing Applications*, May 1998,  
distributed June 25, 1998. [**For Official Use Only**] Requests  
for publication can be made to Naval Facilities Engineering  
Service Center, Security Engineering Division (ESC66),  
1100 23rd Ave., Port Hueneme, CA 93043-4370, Telephone:  
(805)982-1582 (Primary), (805) 982-4817 (Alternate); Fax:  
(805)982-1253

UG-2031-SHR, *Protection Against Terrorist Vehicle Bombs*, May  
1998, distributed June 25, 1998. [**For Official Use Only**]  
Requests for publication can be made to Naval Facilities  
Engineering Service Center, Security Engineering Division  
(ESC66), 1100 23rd Ave, Port Hueneme, CA 93043-4370,  
Telephone: (805)982-15.82 (Primary), (805) 982-4817  
(Alternate); Fax: (805)982-1253

#### **Other Books, Magazines, Magazine Articles, and Newspaper Articles**

Archibald, Rae W., et al., 2002, *Security and Safety in Los Angeles  
High-Rise Buildings after 9/11*. RAND, Santa Monica, CA,  
ISBN: 0-8330-3184-8  
<http://www.rand.org/publications/DB/DB381>

Atlas, Randall I., June 1998, *Designing for Crime and Terrorism*, *Security  
and Technology Design*, Security Technology and Design Magazine  
Reprint Services, Jim Benesh, Telephone: (800)547-7377 x324, Fax:  
(920)568-2244, e-mail: [jim.benesh@cygnuspub.com](mailto:jim.benesh@cygnuspub.com)



Broder, James F., December 15, 1999, *Risk Analysis and the Security Survey, 2nd Edition*, Butterworth-Heinemann, Stoneham, MA, ISBN: 0750670894

Craighead, Geoff, December 2002, *High-Rise Security and Fire Life Safety, 2nd Edition*, Academic Press, ISBN: 0750674555

Crowe, Timothy D., 2000, *Crime Prevention Through Environmental Design: Applications Of Architectural Design And Space Management Concepts (2nd Edition)*, Stoneham, MA, Butterworth-Heinemann, ISBN: 075067198X

Fehr, Stephen C., July 1996, Parking Under Siege in D.C.: U.S. Anti-Terrorism Plan Threatens 360 Spaces, *The Washington Post*, July 13, 1996  
<http://www.washingtonpost.com/wp-adv/archives/advanced.htm>

Fenelly, Lawrence J., June 1997, *Effective Physical Security, 2nd Edition*, Stoneham, MA, Butterworth-Heinemann, ISBN: 0-75-069873-X

Garcia, Mary Lynn, February 23, 2001, *The Design and Evaluation of Physical Protection Systems*, Stoneham, MA, Butterworth-Heinemann, ISBN: 0750673672

Gonchar, Joann, March 2002, Building for a Secure Future: Government Facilities under way incorporate already tough standards, *Engineering News-Record*, March 25, 2002  
<http://www.construction.com/NewsCenter/Headlines/ENR/20020325e.asp>

Greene, R.W., October 2002, *Confronting Catastrophe: A GIS Handbook*, ESRI Press, ISBN: 1589480406

Hart, Sara, March 2002, In the aftermath of September 11, the urban landscape appears vulnerable and random: Architects and consultants focus on risk assessment and security through design, *Architectural Record*, March 2002  
[http://archrecord.construction.com/CONTEDUC/ARTICLES/03\\_02\\_1.asp](http://archrecord.construction.com/CONTEDUC/ARTICLES/03_02_1.asp)

Kowalski, Wladyslaw Jan, P.E., Ph.D., September 26, 2002, *Immune Building Systems Technology*, McGraw-Hill Professional, ISBN: 0-07-140246-2

Nadel, Barbara A, March 1998, Designing for Security, *Architectural Record*, March 1998

[http://www.archrecord.com/CONTEduc/ARTICLES/3\\_98\\_1.asp](http://www.archrecord.com/CONTEduc/ARTICLES/3_98_1.asp)

Owen, David D. and R.S.Means Engineering Staff, *Building Security: Strategies and Costs*, Construction Publishers & Consultants, ISBN: 0-87629-698-3, 2003

Pearson, Robert, September 1997, *Security through Environmental Design, Security and Technology Design*, Security Technology and Design Magazine Reprint Services, Jim Benesh, Telephone: (800) 547-7377 x324; Fax: (920) 568-2244; e-mail: [jim.benesh@cygnuspub.com](mailto:jim.benesh@cygnuspub.com)

Rochon, Donald M., June 1998, *Architectural Design for Security, Security and Technology Design*, Security Technology and Design Magazine Reprint Services, Jim Benesh, Telephone: (800)547-7377 x324; Fax: (920)568-2244; e-mail: [jim.benesh@cygnuspub.com](mailto:jim.benesh@cygnuspub.com)

Security Magazine [on-line magazine]

<http://www.securitymagazine.com>

Security Solutions Online: Access Control and Security Systems [on-line magazine] <http://securitysolutions.com/>

Security Technology and Design [on-line and print magazine]

<http://www.st-and-d.com>

Sidell, Frederick R., et al, 1998, *Jane's Chem-Bio Handbook*, Jane's Information Group, Alexandria, VA, ISBN 0-7106 2568-5  
[http://www.janes.com/company/catalog/chem\\_bio\\_hand.shtml](http://www.janes.com/company/catalog/chem_bio_hand.shtml)

Smith, Keith, November 2000, *Environmental Hazards: Assessing Risk and Reducing Disaster*, Routledge, New York, NY, ISBN 0415224632  
<http://www.routledge-ny.com/books.cfm?isbn=0415224632>

- American Lifelines Alliance  
<http://www.americanlifelinesalliance.org>
- Applied Technology Council  
<http://www.atcouncil.org>
- Battelle Memorial Institute, National Security Program  
<http://www.battelle.org/natsecurity/default.stm>
- Center for Strategic and International Studies (CSIS)  
<http://www.csis.org>
- Centers for Disease Control and Prevention (CDC)/National Institute for Occupational Safety and Health (NIOSH)  
<http://www.cdc.gov/niosh>
- Central Intelligence Agency (CIA)  
<http://www.cia.gov>
- Council on Tall Buildings and Urban Habitat (CTBUH)  
<http://www.ctbuh.org>
- Federal Aviation Administration (FAA)  
<http://www.faa.gov>
- Healthy Buildings International, Inc.  
<http://www.healthybuildings.com>
- Institute of Transportation Engineers  
<http://www.ite.org>
- Interagency Security Committee (ISC) led by the U.S. General Services Administration [*Restricted Access*]  
<http://www.oca.gsa.gov>
- International CPTED [Crime Prevention Through Environmental Design] Association (ICA)  
<http://new.cpted.net/home.amt>
- Lawrence Berkeley National Laboratory (LBNL)  
<http://securebuildings.lbl.gov>

- National Academy of Sciences  
<http://www4.nationalacademies.org/nas/nashome.nsf>
  - Federal Facilities Council (FFC) Standing Committee on Physical Security and Hazard Mitigation  
[http://www7.nationalacademies.org/ffc/Physical\\_Security\\_Hazard\\_Mitigation.html](http://www7.nationalacademies.org/ffc/Physical_Security_Hazard_Mitigation.html)
  - National Research Council  
<http://www.nationalacademies.org/nrc>
- National Defense Industrial Association (NDIA)  
<http://www.ndia.org>
- Public Entity Risk Institute  
<http://www.riskinstitute.org>
- Security Design Coalition  
<http://www.designingforsecurity.org>
- Security Industry Association (SIA)  
<http://www.siaonline.org/>
- Technical Support Working Group  
 (Departments of Defense and State)  
<http://www.tswg.gov>
- U.S. Air Force Electronic System Center (ESC),  
 Hanscom Air Force Base  
<http://eschq.hanscom.af.mil/>
- U.S. Army Soldiers and Biological Chemical Command  
 (SBCCOM): Basic Information on Building Protection  
<http://buildingprotection.sbccom.army.mil>
- U.S. Department of Justice  
<http://www.usdoj.gov>
  - Federal Bureau of Investigation: Terrorism in the United States reports  
<http://www.fbi.gov/publications/terror/terroris.htm>
  - National Institute of Justice (NIJ)  
<http://www.ojp.usdoj.gov/nij>

- Office of Domestic Preparedness (ODP)  
<http://www.ojp.usdoj.gov/odp>
- U.S. Marshals Service (USMS)  
<http://www.usdoj.gov/marshals>

## **The Infrastructure Security Partnership (TISP)**

<http://www.tisp.org>

### **Founding Organizations**

- American Council of Engineering Companies (ACEC)  
<http://www.acec.org>
- The American Institute of Architects (AIA), Security Resource Center  
<http://www.aia.org/security>
- American Society of Civil Engineers (ASCE)  
<http://www.asce.org>
  - Architectural Engineering Institute (AEI) of ASCE  
<http://www.asce.org/instfound/aei.cfm>
  - Civil Engineering Research Foundation (CERF) of ASCE  
<http://www.cerf.org>
  - Structural Engineering Institute (SEI) of ASCE  
<http://www.seinstitute.org>
- Associated General Contractors of America  
<http://www.agc.org>
- Construction Industry Institute  
<http://construction-institute.org>
- Federal Emergency Management Agency (FEMA)  
<http://www.fema.gov>
  - Building Performance Assessment Team  
<http://www.fema.gov/mit/bpat>
  - Human Caused Hazards  
<http://www.fema.gov/hazards>

- Mitigation Planning  
<http://www.fema.gov/fima/planning.shtm>
- Federal Facilities Council – See National Academy of Sciences
- National Institute of Standards and Technology (NIST),  
Building and Fire Research Laboratory  
<http://www.bfrl.nist.gov>
- Naval Facilities Engineering Command  
<http://www.navfac.navy.mil>
  - Naval Facilities Engineering Service Center (NFESC),  
Security Engineering Center of Expertise ESC66  
<http://atfp.nfesc.navy.mil>
- Society of American Military Engineers (SAME)  
<http://www.same.org>
- U.S. Army Corps of Engineers  
<http://www.usace.army.mil>
  - Blast Mitigation Action Group, U.S. Army Corps of  
Engineers Center of Expertise for Protective Design  
<http://bmag.nwo.usace.army.mil>
  - U.S. Army Corps of Engineers, Electronic Security Center  
<http://www.hnd.usace.army.mil/esc>
  - U.S. Army Corps of Engineers, Protective Design Center  
<http://pdc.nwo.usace.army.mil>

#### **Selected Member Organizations**

- Air-Conditioning and Refrigeration Institute, Inc.  
<http://www.ari.org>
- Air Conditioning Contractors of America  
<http://www.acca.org>
- Airport Consultants Council  
<http://www.acconline.org>
- Alliance for Fire & Smoke Containment & Control  
<http://www.afscconline.org>

- American Association of State Highway and Transportation Officials (AASHTO)  
<http://www.transportation.org>
- American Institute of Chemical Engineers, Center for Chemical Process Safety  
<http://www.aiche.org/ccps>
- American Planning Association  
<http://www.planning.org>
- American Portland Cement Alliance  
<http://www.portcement.org/apca>
- American Public Works Association  
<http://www.apwa.net>
- American Railway Engineering & Maintenance of Way Association  
<http://www.arema.org>
- American Society for Industrial Security International (ASIS)  
<http://www.asisonline.org>
- American Society of Heating, Refrigerating, and Air-Conditioning Engineers (ASHRAE)  
<http://www.ashrae.org>
- American Society of Interior Designers  
<http://www.asid.org>
- American Society of Landscape Architects (ASLA)  
<http://www.asla.org>
- American Society of Mechanical Engineers (ASME)  
<http://www.asme.org>
- American Underground Construction Association (AUA)  
<http://www.auca.org> or <http://www.auaonline.org>
- American Water Resources Association (AWRA)  
<http://www.awra.org>
- Associated Locksmiths of America  
<http://www.aloa.org>

- Association of Metropolitan Water Agencies  
<http://www.amwa.net>
- Association of State Dam Safety Officials  
<http://www.damsafety.org>
- Building Futures Council  
<http://www.thebfc.com>
- Building Owners and Managers Association International (BOMA), Emergency Resource Center  
<http://www.boma.org/emergency>
- California Department of Health Services, Division of Drinking Water & Environmental Management  
<http://www.dhs.cahwnet.gov/ps/ddwem>
- Construction Industry Roundtable  
<http://www.cirt.org>
- Construction Innovation Forum  
<http://www.cif.org>
- Construction Specifications Institute  
<http://www.csinet.org>
- Construction Users Roundtable  
<http://www.curt.org>
- Defense Threat Reduction Agency (DTRA)  
<http://www.dtra.mil>
- Design-Build Institute of America  
<http://www.dbia.org>
- Drexel (University) Intelligent Infrastructure & Transportation Safety Institute  
<http://www.di3.drexel.edu>
- Federal Highway Administration  
<http://www.fhwa.dot.gov>
- Florida Department of Transportation, Emergency Management Office  
<http://www11.myflorida.com/safety/Emp/emp.htm>



or

Florida Department of Community Affairs, Division of  
Emergency Management

[http://www.floridadisaster.org/bpr/EMTOOLS/Severe/  
terrorism.htm](http://www.floridadisaster.org/bpr/EMTOOLS/Severe/terrorism.htm)

or

[http://www.dca.state.fl.us/bpr/EMTOOLS/CIP/critical\\_  
infrastructure\\_protecti.htm](http://www.dca.state.fl.us/bpr/EMTOOLS/CIP/critical_infrastructure_protecti.htm)

- George Washington University, Institute for Crisis, Disaster,  
and Risk Management

<http://www.cee.seas.gwu.edu>

or

<http://www.seas.gwu.edu/~icdm>

- Homeland Protection Institute, Ltd.

<http://www.hpi-tech.org>

- Inland Rivers Ports and Terminals

<http://www.irpt.net>

- Institute of Electrical and Electronics Engineers, Inc. - USA

<http://www.ieeeusa.org> or [http://www.ieee.org/portal/  
index.jsp](http://www.ieee.org/portal/index.jsp)

- International Association of Foundation Drilling

<http://www.adsc-iafd.com>

- International Code Council (ICC)

<http://www.intlcode.org>

Consolidates services, products, and operations of BOCA  
(Building Officials and Code Administrators), ICBO  
(International Conference of Building Officials) and SBCCI  
(Southern Building Code Congress International) into one  
member service organization — the International Code Council  
(ICC) in January 2003.

- International Facility Management Association (IFMA)

<http://www.ifma.org>

- Market Development Alliance of the FRP Composites Industry

<http://www.mdacomposites.org>

- Multidisciplinary Center for Earthquake Engineering Research  
<http://mceer.buffalo.edu>
- National Aeronautics and Space Administration  
<http://www.nasa.gov>
- National Capital Planning Commission (NCPC)  
<http://www.ncpc.gov>
  - Security and Urban Design  
[http://www.ncpc.gov/planning\\_init/security.html](http://www.ncpc.gov/planning_init/security.html)
- National Center for Manufacturing Sciences  
<http://www.ncms.org>
- National Concrete Masonry Association  
<http://www.ncma.org>
- National Conference of States on Building Codes and Standards  
<http://www.ncsbc.org>
- National Council of Structural Engineers Associations (NCSEA) <http://www.ncsea.com> or <http://dwp.bigplanet.com/engineers/homepage>
- National Crime Prevention Institute  
<http://www.louisville.edu/a-s/ja/ncpi/courses.htm>
- National Fire Protection Association  
<http://www.nfpa.org>
- National Institute of Building Sciences (NIBS)  
<http://www.nibs.org> and <http://www.wbdg.org>
- National Park Service, Denver Service Center  
<http://www.nps.gov/dsc>
- National Precast Concrete Association  
<http://www.precast.org>
- National Wilderness Training Center, Inc.  
<http://www.wildernesstraining.net>

- New York City Office of Emergency Preparedness  
<http://www.nyc.gov/html/oem>
- Ohio State University  
<http://www.osu.edu/homelandsecurity>
- Pentagon Renovation Program  
<http://renovation.pentagon.mil>
- Portland Cement Association (PCA)  
<http://www.portcement.org>
- Primary Glass Manufacturers Council  
<http://www.primaryglass.org>
- Protective Glazing Council  
<http://www.protectiveglazing.org>
- Protective Technology Center at Penn State University  
<http://www.ptc.psu.edu>
- SAVE International  
<http://www.value-eng.org>
- Society of Fire Protection Engineers  
<http://www.sfpe.org>
- Southern Building Code Congress, International  
<http://www.sbcci.org>
- Sustainable Buildings Industry Council  
<http://www.sbicouncil.org>
- Transit Standards Consortium  
<http://www.tsconsortium.org>
- Transportation Research Board/Marine Board  
<http://www.trb.org>
- Transportation Security Administration - Maritime and Land  
<http://www.tsa.dot.gov>
- U.S. Air Force Civil Engineer Support Agency  
<http://www.afcesa.af.mil>

- U.S. Coast Guard  
<http://www.uscg.mil>
- U.S. Department of Energy  
<http://www.energy.gov>
  - Sandia National Laboratories (SNL)  
<http://www.sandia.gov>
    - Architectural Surety Program  
<http://www.sandia.gov/archsur>
    - Critical Infrastructure Protection Initiative  
[http://www.sandia.gov/LabNews/LN02-11-00/steam\\_story.html](http://www.sandia.gov/LabNews/LN02-11-00/steam_story.html)
- U.S. Department of Health and Human Services  
<http://www.hhs.gov>
- U.S. Department of Veterans Affairs (VA)  
<http://www.va.gov/facmgt>
- U.S. Environmental Protection Agency (EPA), Chemical Emergency Preparedness and Prevention Office (CEPPO)–Counter-terrorism  
<http://www.epa.gov/swercepp/cntr-ter.html>
- U.S. General Services Administration (GSA)  
<http://www.gsa.gov>
  - Office of Federal Protective Service (FPS) of GSA  
[http://www.gsa.gov/Portal/content/orgs\\_content.jsp?contentOID=117945&contentType=1005&P=1&S=1](http://www.gsa.gov/Portal/content/orgs_content.jsp?contentOID=117945&contentType=1005&P=1&S=1)
  - Office of Public Building Service (PBS) of GSA  
[http://www.gsa.gov/Portal/content/orgs\\_content.jsp?contentOID=22883&contentType=1005&PPzz=1&S=1](http://www.gsa.gov/Portal/content/orgs_content.jsp?contentOID=22883&contentType=1005&PPzz=1&S=1)
  - Office of the Chief Architect of GSA  
[http://www.gsa.gov/Portal/content/orgs\\_content.jsp?contentOID=22899&contentType=1005](http://www.gsa.gov/Portal/content/orgs_content.jsp?contentOID=22899&contentType=1005)  
and  
<http://www.oca.gsa.gov>

- U.S. Green Building Council  
<http://www.usgbc.org>
- U.S. Marine Corps Headquarters  
<http://www.usmc.mil>
- U.S. Society on Dams  
<http://www.ussdams.org>
- University of Missouri, Department of Civil & Environmental Engineering, National Center for Explosion Resistant Design  
<http://www.engineering.missouri.edu/explosion.htm>
- Virginia Polytechnic Institute and State University  
<http://www.ce.vt.edu>
- Water and Wastewater Equipment Manufacturers Association  
<http://www.wwema.org>

### **The Partnership for Critical Infrastructure (PCIS)**

<http://www.pcis.org>

Note: Involved mainly with information systems and not building real property.

#### **Government**

- Department of Commerce Critical Infrastructure Assurance Office (CIAO)  
<http://www.ciao.gov>
- Department of Energy (DOE)  
<http://www.energy.gov>
- Department of Homeland Security  
<http://www.whitehouse.gov/deptofhomeland>
- National Infrastructure Protection Center (NIPC)  
<http://www.nipc.gov>

#### **Private Sector**

- Anser Institute for Homeland Security (ANSER)  
<http://www.homelandsecurity.org>

- CERT® Coordination Center (CERT/CC)  
<http://www.cert.org>
- Electronic Warfare Associates (EWA)  
<http://www.ewa.com>
- Information Technology Association of America (ITAA)  
<http://www.itaa.org>
- The Institute for Internal Auditors (IIA)  
<http://www.theiia.org>
- National Cyber Security Alliance (Alliance)  
<http://www.staysafeonline.info>
- North American Electric Reliability Council (NERC)  
<http://www.nerc.com>
- SANS Institute (SANS - SysAdmin, Audit, Network, Security)  
<http://www.sans.org>
- The Financial Services Roundtable Technology Group (BITS)  
<http://www.bitsinfo.org>
- The U.S. Chamber of Commerce, Center for Corporate Citizenship (CCC)  
<http://www.uschamber.com/ccc>

#### **Selected States and Local Organizations**

- Association of Metropolitan Water Agencies  
<http://www.amwa.net>
- The Council of State Governments (CSG)  
<http://www.csg.org>
- International Association of Emergency Managers (IAEM)  
<http://www.iaem.com>
- National Association of State CIOs (NASCIO)  
<http://www.nascio.org>
- National Emergency Managers Association (NEMA)  
<http://www.nemaweb.org>

- National Governor's Association (NGA)  
<http://www.nga.org>
- The National League of Cities (NLC)  
<http://www.nlc.org>

